NIST Special Publication
NIST SP 800-50r1 ipd

Building a Cybersecurity and Privacy Learning Program

Initial Public Draft

Marian Merritt
Susan Hansche
Brenda Ellis
Kevin Sanchez-Cherry
Julie Nethery Snyder
Donald Walden

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

17 **NIST Special Publication**
18 **NIST SP 800-50r1 ipd**

19 # Building a Cybersecurity and
20 # Privacy Learning Program

21
22 Initial Public Draft

Marian Merritt
Applied Cybersecurity Division
Information Technology Laboratory

Susan Hansche
Cybersecurity and Infrastructure
Security Agency
Department of Homeland Security

Brenda Ellis
National Aeronautics and Space
Administration

Kevin Sanchez-Cherry
Office of the Chief Information Officer
Department of Transportation

Julie Nethery Snyder
MITRE

Donald Walden
Internal Revenue Service

1
2 This publication is available free of charge from:
3 https://doi.org/10.6028/NIST.SP.800-50r1.ipd

4 August 2023

5
6 U.S. Department of Commerce
7 *Gina M. Raimondo, Secretary*

8 National Institute of Standards and Technology
9 *Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

10 Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in
11 this paper in order to specify the experimental procedure adequately. Such identification does not imply
12 recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or
13 equipment identified are necessarily the best available for the purpose.

14 There may be references in this publication to other publications currently under development by NIST in
15 accordance with its assigned statutory responsibilities. The information in this publication, including concepts and
16 methodologies, may be used by federal agencies even before the completion of such companion publications. Thus,
17 until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain
18 operative. For planning and transition purposes, federal agencies may wish to closely follow the development of
19 these new publications by NIST.

20 Organizations are encouraged to review all draft publications during public comment periods and provide feedback
21 to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
22 https://csrc.nist.gov/publications.

23 **Authority**
24 This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal
25 Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283.
26 NIST is responsible for developing information security standards and guidelines, including minimum requirements
27 for federal information systems, but such standards and guidelines shall not apply to national security systems
28 without the express approval of appropriate federal officials exercising policy authority over such systems. This
29 guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.
30
31 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding
32 on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be
33 interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or
34 any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and
35 is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

36 **NIST Technical Series Policies**
37 Copyright, Use, and Licensing Statements
38 NIST Technical Series Publication Identifier Syntax

39 **Publication History**
40 Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added upon final publication.]
41 Supersedes NIST Series XXX (Month Year) DOI [Will be added upon final publication.]

42 **How to Cite this NIST Technical Series Publication:**
43 Merritt M, Hansche S, Ellis B, Sanchez-Cherry K, Snyder JN, Walden D (2023) Building a Cybersecurity and
44 Privacy Learning Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
45 Publication (SP) NIST SP 800-50r1 ipd. https://doi.org/10.6028/NIST.SP.800-50r1.ipd

46 **Author ORCID iDs**
47 Marian Merritt: 0000-0002-2116-8959

48 **Public Comment Period**
49 August 28, 2023 – October 27, 2023

50 **Submit Comments**
51 sp800-50-comments@nist.gov
52
53 National Institute of Standards and Technology
54 Attn: Applied Cybersecurity Division, Information Technology Laboratory
55 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

56 **All comments are subject to release under the Freedom of Information Act (FOIA).**

Abstract

This publication provides guidance for federal agencies and organizations to develop and manage a lifecycle approach to building a cybersecurity and privacy learning program (hereafter referred to as CPLP). The approach is intended to address the needs of large and small organizations as well as those building an entirely new program. The information leverages broadly accepted standards, regulations, legislation, and best practices. The recommendations are customizable and may be implemented as part of an organization-wide process that manages awareness, training, and education programs for a diverse set of employee audiences. The guidance also includes suggested metrics and evaluation methods in order that the program be regularly improved and updated as needs will evolve.

Keywords

awareness; cybersecurity; education; learning program; privacy; role-based; training.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective cybersecurity and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

80 **Call for Patent Claims**

81 This public review includes a call for information on essential patent claims (claims whose use
82 would be required for compliance with the guidance or requirements in this Information
83 Technology Laboratory (ITL) draft publication). Such guidance or requirements may be directly
84 stated in this ITL Publication or by reference to another publication. This call also includes
85 disclosure, where known, of the existence of pending U.S. or foreign patent applications relating
86 to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

87 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
88 in written or electronic form, either:

89 a) assurance in the form of a general disclaimer to the effect that such party does not hold
90 and does not currently intend holding any essential patent claim(s); or

91 b) assurance that a license to such essential patent claim(s) will be made available to
92 applicants desiring to utilize the license for the purpose of complying with the guidance
93 or requirements in this ITL draft publication either:

94 i. under reasonable terms and conditions that are demonstrably free of any unfair
95 discrimination; or

96 ii. without compensation and under reasonable terms and conditions that are
97 demonstrably free of any unfair discrimination.

98 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
99 on its behalf) will include in any documents transferring ownership of patents subject to the
100 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
101 the transferee, and that the transferee will similarly include appropriate provisions in the event of
102 future transfers with the goal of binding each successor-in-interest.

103 The assurance shall also indicate that it is intended to be binding on successors-in-interest
104 regardless of whether such provisions are included in the relevant transfer documents.

105 Such statements should be addressed to: sp800-50-comments@nist.gov

106   **Table of Contents**

181   **List of Tables**

183   **List of Figures**

188

189 **Acknowledgments**

196

Executive Summary

Ensuring that an organization's workforce is aware of and prepared to respond appropriately and effectively to cybersecurity and privacy risk is an important effort that requires a strategic approach based on thoughtful planning, resource considerations, and leadership-driven decision making. This long-awaited update to the 2003 NIST Special Publication (SP) 800-50, *Building an Information Technology Security Awareness and Training Program,* provides guidance that includes awareness, role-based training, and education programs. These programs combine to create an overall Cybersecurity and Privacy Learning Program (CPLP) that supports federal requirements and incorporates industry-recognized best practices for risk management.

Legislative authority for the creation and maintenance of this ~~S~~pecial ~~P~~ublication is derived from the National Defense Authorization Act of 2021 ~~(NDAA) [2]~~.

In addition to the statutory responsibilities under FISMA, this Special Publication supports the National Defense Authorization Act of 2021 (NDAA) [2], *Development of Standards and Guidelines for Improving Cybersecurity Workforce of Federal Agencies* to "publish standards and guidelines for improving cybersecurity awareness of employees and contractors of Federal agencies"[1] Including privacy as a foundational element in this Program reflects the guidance found in the 2016 update to OMB's Circular A-130:

> …it also emphasizes the role of both privacy and security in the federal information life cycle. Importantly, the inclusion of privacy represents a shift from viewing security and privacy requirements as merely compliance exercises to understanding security and privacy as crucial and related elements of a comprehensive, strategic, and continuous risk-based program at federal agencies. [1]

Additionally, this update includes elements previously found in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* [6]. Previously, NIST SP 800-16 [6] identified the federal agency and organizational work roles that required specialized training for cybersecurity tasks and skills. The relevant content from NIST SP 800-16 has been incorporated into this publication or has been included in NIST SP 800-181r1 [3]. As a result, NIST SP 800-16 will be withdrawn upon the release of this publication

Everyone in an organization has a role to play in the success of an effective cybersecurity and privacy program. For those whose information technology, cybersecurity, or cybersecurity-related job responsibilities require additional or specific training, the NICE Workforce Framework for Cybersecurity (NICE Framework)[2] [3] identifies the specific knowledge and skills necessary to perform tasks associated with work roles in these areas.[3]

---

[1] Section 9402 of FY 21 NDAA, *Development of Standards and Guidelines for Improving Cybersecurity Workforce of Federal Agencies*, amends the NIST Act as follows: "(b): PUBLICATION OF STANDARDS AND GUIDELINES ON CYBERSECURITY AWARENESS. Not later than three years after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall publish standards and guidelines for improving cybersecurity awareness of employees and contractors of federal agencies."
[2] National Initiative for Cybersecurity Education (NICE) is led by NIST in the US Department of Commerce.
[3] As of the time of development of this publication, NIST is in the process of a privacy workforce development effort to create a privacy companion to NICE.

231   Users of this publication will find guidance on the steps necessary to:

232   • Build an effective CPLP for all organizational personnel, including employees and
233   contractors

234   • Identify personnel who require advanced training

235   • Create a methodology for evaluating the program

236   • Engage in ongoing improvement to the program

237   Throughout each section, there are recommendations to enable a program to continually evolve
238   and improve, thereby minimizing risks to the organization.

239   This document identifies the phases in the management of a CPLP and is organized as follows:

240   • Section 1: Introduction

241   • Section 2: The CPLP Strategy and Planning Process

242   • Section 3: Analyzing and Designing the CPLP

243   • Section 4: Development and Implementation of the CPLP

244   • Section 5: Assessing and Improving the CPLP

1.   Introduction

Ongoing cybersecurity and privacy risks require continuous attention. An organization must enlist participation from everyone to reduce and manage its risk. A key component of an organization's cybersecurity and privacy plans are the Learning Program(s), which helps to build an understanding of risks and explain everyone's role in identifying, responding to, and managing those risks. While Learning Programs vary in each organization, there are fundamental shared elements that can be utilized to create the Cybersecurity and Privacy Learning Program (CPLP) strategy and establish support for implementation, evaluation, and reporting activities.

For ease of use, the remainder of this document will use the term "CPLP" to refer to all elements of cybersecurity and privacy awareness activities and campaigns, including awareness training, practical exercises (e.g. table-top exercises, cyber ranges, or phishing campaigns), topic-based training, role-based training, and education programs.

The previous version of this Special Publication defined awareness, training, and education as separate elements in a learning continuum. Research efforts [10] conducted with Federal Government training managers have shown that these terms have different meanings and can lead to confusion when describing the broader purpose of building a CPLP. While managers may refer to programs as "awareness and training" or "awareness training," the terms are applied inconsistently across organizations. Regardless of what the organization calls its program, the overarching goal is to provide opportunities for learning at all levels or stages of one's career. It is about creating programs where learning can take place.

NIST SP 800-181r1, *NICE Workforce Framework for Cybersecurity (NICE Framework)* [3], refers to an individual who is acquiring specialized knowledge or developing skill as a "learner." This terminology is useful here as well, so this document will refer to the program as a CPLP or CPLPs, as some organizations may require multiple Programs. Additionally, some organizations may have separate CPLPs.

1.1.   Purpose

This document provides guidelines for building and maintaining comprehensive cybersecurity and privacy learning programs (CPLPs) that include awareness activities and campaigns, awareness training, practical exercises, topic-based training, role-based training, and education programs. The document includes guidance on how an organization can create a strategic program plan and ensure that there are appropriate resources to meet the organization's learning goals.

This publication is intended to serve a diverse audience, including:

- **Workforce and learning professionals:** This group includes human resource planners, training coordinators, curriculum developers, course developers, and those responsible for developing, presenting, and evaluating the training. This document will assist training professionals with the following: understanding cybersecurity and privacy requirements, knowledge, and skills; evaluating the course quality; obtaining the appropriate courses and materials; developing or customizing courses and materials; and tailoring their teaching approaches to achieve the desired learning objectives. Workforce and learning professionals includes:

286   o Individuals associated with the design, development, implementation, assessment,
287   operation, management, and ongoing improvements to the CPLPs for federal agencies
288   and organizations

289   o Individuals with human resources and talent management responsibilities as well as
290   oversight responsibilities for contractors and training programs

291   o Individuals responsible for the CPLPs, training professionals, and managers, such as
292   Chief Learning Officers and curriculum developers

293   • **Leadership and management:** This includes all levels of management who are
294   responsible for staff training needs, prioritizing the use of training resources, identifying
295   training gaps, and evaluating training effectiveness within the workspace. Leadership and
296   management includes:

297   o Individuals with information system oversight or governance responsibilities, such as
298   senior leaders, risk executives, authorizing officials, chief information officers (CIO),
299   chief information security officers (CISO), data management officers, and chief
300   privacy officers (CPO)

301   o Individuals with cybersecurity and privacy management responsibilities (e.g.,
302   managing programs and projects and ensuring that staff members have the
303   appropriate knowledge and skills to perform their work roles), including program and
304   project managers, cybersecurity managers, and security operation managers

305   • **Cybersecurity and privacy specialists:** This group includes workforce members who
306   are responsible for assisting in identifying CPLP activities and aids as a subject-matter
307   expert (SME), meeting the requirements of the roles or job functions, identifying learning
308   gaps and needs within the organization's cybersecurity and privacy program, determining
309   necessary customizations, and developing a compliance baseline for the organization.

310

Key Considerations for Cybersecurity and Privacy Learning Programs [4]

- Develop, maintain, and implement mandatory organization-wide cybersecurity and privacy learning programs for all members of the workforce that support enterprise cybersecurity and privacy goals and objectives.
- Ensure that the CPLP aligns with established rules of behavior and is consistent with applicable policies, standards, and guidelines.
- Apprise the workforce of available cybersecurity and privacy resources, such as products, techniques, or expertise.
- Provide foundational as well as more advanced levels of cybersecurity and privacy training to the workforce and ensure that measures are in place to assess the knowledge and skill of participants.
- Identify who needs specialized cybersecurity and privacy training based on assigned cybersecurity and privacy roles and responsibilities.

---

[4] This text is adapted from OMB A-130, Appendix I, Section 4.h, and is meant to accommodate the needs of any organization, not just federal agencies and organizations.

311

1.2. Scope

The scope of this guide covers the steps that an organization should take to create a strategy and program plan, including the design, development, implementation, and maintenance of a CPLP as part of an enterprise cybersecurity and privacy program. The scope includes identifying the learning needs for the personnel of an organization, from federal and contract employees to supervisors, functional managers, and executive-level managers. As noted previously, CPLPs are inclusive of various other programs, including awareness programs, social engineering campaigns, new hire training, annual training, technical training and requirements for role-based training, and other relevant learning activities. These learning activities may be conducted within the organization or necessitate access to external resources, such as courses, certificates, and advanced programs.

1.3. The CPLP Life Cycle

The CPLP must have an actively managed plan, which requires attention and adjustment over time, throughout the Life Cycle. Learning Program Managers should carefully and thoughtfully outline, discuss, review, and document the CPLP's goals and available options. When the owners of the organization's CPLP adopt an effective strategy and develop a proper planning approach with measurement and feedback through the year, the entire organization remains connected to the CPLP objectives. **Fig. 1** shows the various phases of building and managing a Learning Program: Plan and Strategy, Analysis and Design, Development and Implementation, Assessment and Improvement.

332

Fig. 1. The Cybersecurity and Privacy Learning Program life cycle

334 These phases can occur in sequence or simultaneously. At any time during the life cycle, the
335 Learning Program Manager and team can develop curriculum, evaluate instructor feedback, send
336 out practical exercise email quizzes, design posters for awareness, or develop a presentation for
337 senior leadership. Consider this diagram a reminder of the breadth of work.

338 In a broad sense, the CPLP is a valued element of the organization's learning culture. To be
339 effective, the CPLP must be linked to organizational goals and viewed as adaptive, continuous,
340 and evolving. In a learning organization, personnel can expand and enhance their current
341 capabilities to understand and meet new mission requirements. Personnel are respected for their
342 ability to create and inspire others and are active in creating life-long learning achievements. If
343 an organization offers other learning programs (e.g., career development, leadership, and
344 executive development), the CPLP needs to be similarly integrated into the enterprise-wide
345 learning structure.

1.4.   Developing a Cybersecurity and Privacy Culture

347 Establishing a cybersecurity and privacy culture is an important component of establishing a
348 successful CPLP. The culture of the organization should emphasize, reinforce, and drive its
349 desired behaviors toward cybersecurity and privacy. When a CPLP is valued in the
350 organization's culture, the ability to address risks is increased. The organization's leaders are
351 strategically valuable in establishing the CPLP as a significant component of managing risk.
352 Leaders create a learning culture by supporting and championing learning activities, from
353 awareness campaigns to role-based training. They help to set the tone for the entire organization.

354   The Government Accountability Office (GAO)[5] noted that in FY 2021 federal civilian agencies
355   reported 32,511 information security incidents. The largest identified percentage (31 %) of
356   reported incidents were from improper usage and 9 % were from email phishing (46 % are
357   shown as "unknown"). Improper usage is defined as "any incident resulting from violation of an
358   organization's acceptable usage policies by an authorized user." While these statistics may
359   change from year to year, the high level of incidents from improper usage demonstrates the need
360   for CPLPs. To reduce improper use, it is crucial that every user receives training on the rules of
361   behavior and their role in reducing the risks associated with the organization's data and systems.

362   To support an inclusive culture, the approach in any CPLP should focus on helping the learner
363   understand their role in the organization with respect to their cybersecurity and privacy
364   responsibilities. The content should indicate to the learner that they are a valued participant in
365   helping the organization manage risk. The workforce appreciates that they will contribute to the
366   organization's positive cybersecurity and privacy culture with the knowledge and skills they
367   acquire by participating in the CPLP. The stereotypes of "hackers in hoodies" and myth of
368   "technologies solving the problem" are dated. People are an organization's greatest asset. Any
369   effective learning activity can be incorporated into the CPLP when it is respectful and inclusive.

370   A cybersecurity and privacy culture supports an environment where – from executives to every
371   user – the workforce is well-versed in the cybersecurity and privacy risk management needs,
372   expectations, and values of their organization and understands their roles and responsibilities for
373   meeting them. An organization supports an effective cybersecurity and privacy culture when it
374   understands the needs of the workforce and provides education and training to help employees
375   and contractors learn expected cybersecurity and privacy behaviors.

376   Organizations and system owners must develop a CPLP approach that champions every user's
377   responsibility to protect information and assets. It is important to recognize how new
378   technologies and new risks will continue to necessitate an organization-wide approach to
379   managing cybersecurity and privacy risks. The NIST Cybersecurity Framework [4], Privacy
380   Framework [5], and the Risk Management Framework (RMF) [7] highlight the importance of
381   awareness and training for personnel.

382   **1.5.   Relationship Between Cybersecurity and Privacy**

383   While cybersecurity and privacy are independent and separate disciplines, some of their
384   objectives are overlapping and complementary. Cybersecurity programs are responsible for
385   protecting information and information systems as well as operational technologies from
386   unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized
387   system activity or behavior) in order to provide confidentiality, integrity, availability and safety.
388   Privacy programs are responsible for managing the risks to individuals associated with data
389   processing throughout the information life cycle[6] in order to provide predictability,
390   manageability, and disassociability, as well as ensuring compliance with applicable privacy
391   requirements. Managing cybersecurity risk contributes to managing privacy risk. However,
392   managing cybersecurity risk alone is not sufficient, as privacy risks can also arise by means
393   unrelated to cybersecurity incidents, as illustrated by **Fig. 2**.

---

[5] See https://www.gao.gov/cybersecurity.
[6] "The information life cycle describes the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion [OMB A-130]"
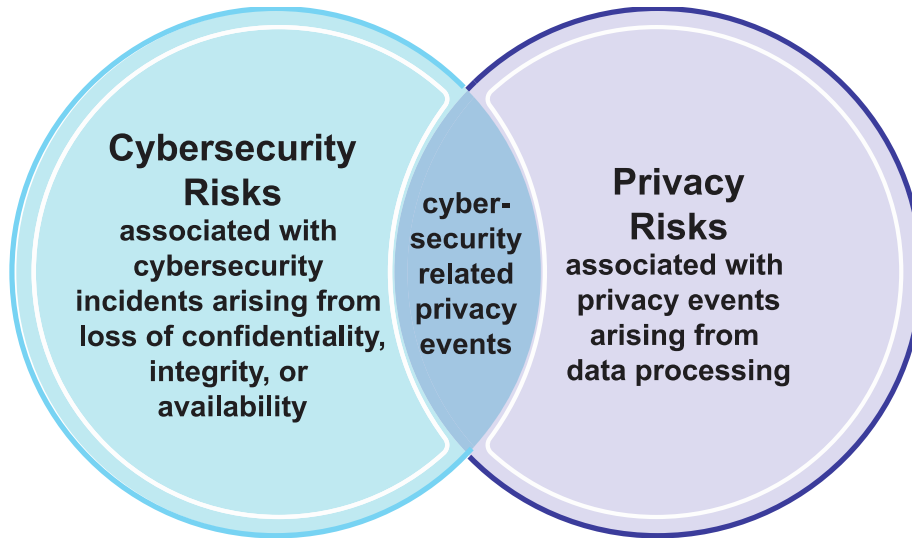
Fig. 2. Cybersecurity and privacy risk relationship [5]

For example, the Privacy Act requires federal agencies to disclose much of the information about individuals in their records when the individual requests it. However, if the organization's cybersecurity posture does not allow for the efficient sharing of information, individuals risk privacy violations because they may experience problems or harms resulting from their inability to know what information is held about them.

Providing the workforce with a general understanding of the different origins of cybersecurity and privacy risks is important for enabling them to effectively address the risks they encounter in their daily activities. For example, all members of the workforce will need training that helps them understand when a privacy event has occurred, and incident response professionals will need training that helps them determine when a cybersecurity incident may also be a privacy event, which often requires additional procedures when responding (e.g., determining if an unsecured site resulted in an actual data breach of PII). Organizations can benefit from taking a coordinated approach to developing CPLPs and have the flexibility to determine how to effectively do so to meet the organization's needs.[7]

Once an organization understands the relationship between cybersecurity and privacy in its context, it can determine its approach to developing both integrated and cybersecurity- or privacy-specific learning activities based on the relevant topics and workforce roles in the environment. For example, the organization can determine how to effectively:

- Associate learning tracks with work roles and job performance

- Describe its approach to managing cybersecurity and privacy risk in a way that aligns with enterprise risk management capabilities

- Incorporate lessons learned from cybersecurity and privacy risk, audit findings, incidents, or events, or changes to governance documents (e.g., laws, regulations, policies, and standards) into general and role-based training

---

[7] Role-based privacy training should address the full scope of privacy risks, as depicted in **Fig. 1**. For federal agencies, role-based privacy training addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, Privacy Act statements, contracts, information sharing agreements, memoranda of understanding, or other documentation.

419 • Institute learning activities that are appropriate for both internal and external members of the
420 workforce, including contractors and third parties

421 • Identify learning obligations in contracts and agreements

422 • Identify and track metrics to assess the effectiveness of learning efforts (e.g., determining whether
423 the number of a certain type of incident or event decreases after a targeted awareness campaign)

1.6. Privacy Risk Management Concepts to Emphasize

425 Members of the workforce who are in roles that can impact privacy must also have a clear
426 understanding of how to identify and address privacy risk that may arise.

427 The NIST Privacy Framework [5] provides a common language for understanding, managing,
428 and communicating privacy risk. Just as the workforce considers the risk associated with security
429 incidents, they must also consider *privacy events* – the potential problems that could arise from
430 system, product, or service operations with data, whether in digital or non-digital form, through a
431 complete life cycle from data collection through disposal. Privacy problems can arise from an
432 individual's direct use of a product. Some problems can also arise simply from individuals'
433 interactions with systems, products, and services, even when the data being processed is not
434 directly linked to identifiable individuals. The problems that individuals can experience as a
435 result of data processing can be expressed in various ways. The NIST Privacy Framework
436 describes them as ranging from dignity-type effects (e.g., embarrassment or stigmas) to more
437 tangible harms (e.g., discrimination, economic loss, or physical harm).[8]

438 As a result of the problems that individuals experience, an organization may in turn experience
439 impacts such as noncompliance costs, revenue loss arising from customer abandonment of
440 products and services, or harm to its external brand reputation or internal culture. Organizations
441 commonly manage these types of impacts at the enterprise risk management level. By connecting
442 problems that individuals experience to these well-understood organizational impacts,
443 organizations can bring privacy risk into parity with other risks that they manage in their broader
444 portfolio and drive more informed decision-making about resource allocation to strengthen
445 privacy programs. **Fig. 3** illustrates the relationship between privacy risk and organizational risk.

---

[8] The NIST Catalog of Problematic Data Actions and Problems provides examples of privacy problems that individuals may face and is available
at https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-
PRAM/catalog-PDAP.md.
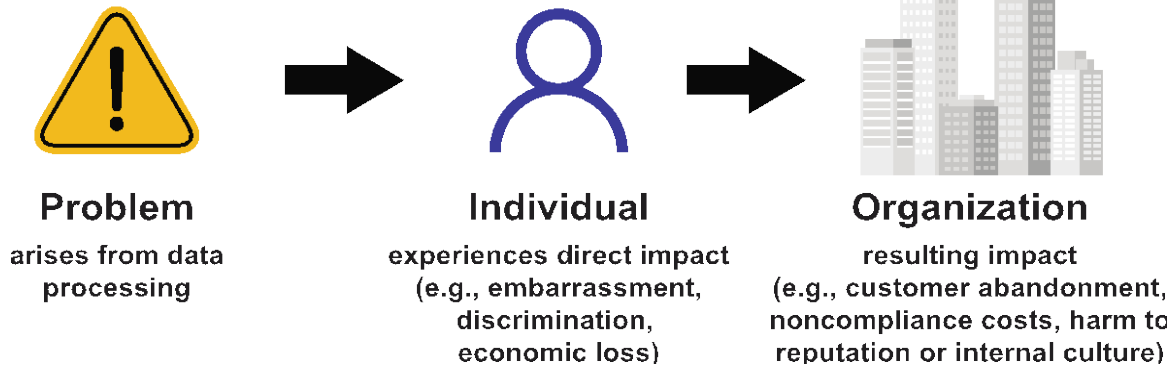
446
447
448   **Fig. 3.** Relationship between privacy risk and organizational risk [5]

449   Privacy Learning Programs are most effective when they help the workforce understand both the
450   direct impacts that organizational activities can have on individuals and the resulting impacts that
451   privacy risks can have on the organization. For example, the program can address the types of
452   impacts that an individual may experience from the loss of personal information (e.g., identity
453   theft) and the resulting consequences to the organization (e.g., costs associated with a data
454   breach, such as providing credit monitoring to customers, loss of trust in the organization, or
455   decline in value of stock share price).

456   ## 1.7.   Coordinating Cybersecurity and Privacy Learning Efforts

457   An organization's CPLP should coordinate with the cybersecurity and privacy program(s). As
458   discussed in Section 1.4, cybersecurity and privacy risk management practices may overlap with
459   learning needs. With limited resources, duplicating efforts will negatively affect one or both
460   programs. In cases with an integrated cybersecurity and privacy program, this is less likely to be
461   an issue.

462

463   ## 1.8.   Roles and Responsibility

464   While it is important to understand the policies that require agencies to develop and implement
465   CPLPs, it is also crucial that organizations understand who has responsibility for cybersecurity
466   and privacy learning. This section identifies and describes those within an organization who are
467   responsible for ensuring that the workforce has access to and completes their cybersecurity and
468   privacy learning.

469   It may be useful to refer to related NIST Special Publications for consistent references to the
470   crucial roles in an organization that have a vested interest in the implementation of a robust
471   CPLP. NIST SP 800-37 [7] identifies the typical roles associated with these programs. Since
472   terminology may vary by organization, it can be useful to refer to the NICE Framework as a
473   complementary tool for identifying those with responsibilities for managing the CPLP as well as
474   those who require additional training.

475 The size, maturity, and resources of CPLPs can also vary widely, even within components of the
476 same organization. The roles and responsibilities for key positions in a CPLP should be
477 documented to help ensure the most effective use of resources and enable the program to mature
478 to its desired state.

1.8.1. Organization Head

480 Organization heads must prioritize the development of an effective CPLP. This includes
481 implementing a viable cybersecurity and privacy program with a strong learning component.
482 Organization heads should:

- 483 Designate leadership roles to manage the organization's cybersecurity and privacy
484 learning programs. Empower these roles to develop the strategic direction for the learning
485 program; performance goals and objectives are written; and performance metrics are
486 reviewed and managed. Learning Program Managers, who are responsible for the
487 analysis, design, development and delivery of the CPLP, are identified and given
488 resources adequate to meet the performance goals and objectives

- 489 Ensure that an agency- or organization-wide cybersecurity and privacy program is
490 implemented, well-supported by resources, including personnel and funding, and
491 effective at reducing and managing risk

- 492 Ensure that the agency or organization has enough sufficiently knowledgable and skilled
493 personnel to support its programs and resources and individuals's privacy

1.8.2. Senior Leadership

495 FISMA [9], OMB A-130 [1], and various other regulations designate the responsibility for
496 ensuring cybersecurity and privacy learning programs to certain senior official positions, such as
497 the Chief Information Officer, Chief Privacy Officer, Chief Information Security Officer, and
498 Chief Data Officer. These roles are tasked with setting strategic direction, ensuring resources are
499 available, and overseeing personnel with significant responsibilities for cybersecurity and
500 privacy, including the roles found in the NICE Framework [3]. Senior officials should work with
501 their Learning Program Managers to:

- 502 Establish an overall strategy for the CPLPs

- 503 Provide resource support for the implementation of the CPLPs' life cycle phases

- 504 Recognize any deficiencies in the organizational culture, risks, or requirements and
505 address them with appropriate program funding and management

506 In addition, senior leaders must champion workforce requirements, such as:

- 507 Leading by example and participating in their own CPLP training, as required.

- 508 Identifying who has cybersecurity and privacy responsibilities and documenting it in
509 position descriptions or other relevant work and performance requirement statements

- 510 Identifying relevant learning requirements and documenting it in individual development
511 plans or other career pathway documentation

512   • Establishing policies and procedures for learning programs and documenting it in the
513   organizational records

514   A recommended approach for an agency or organization would be to form a Senior Leadership
515   Committee that meets regularly with Learning Program Managers to discuss strategy and provide
516   resource support. The Learning Program Manager will provide the Senior Leadership Committee
517   with regular reports on the Learning Program's performance throughout the year.

1.8.3. Learning Program Manager

519   Learning Program Managers have tactical-level responsibilities for the CPLP. In this role, the
520   Program Manager should, in consultation with the curriculum development professionals and
521   curriculum instruction team:

522   • Facilitate the development of learning material that is appropriate and timely for the
523   intended audiences

524   • Provide effective mechanisms for deploying the learning material so that it reaches the
525   intended audience

526   • Offer users and managers an effective way of providing feedback on the learning material
527   and its presentation

528   • Oversee periodic reviews and update the learning material when necessary

529   • Assist in establishing a tracking and reporting strategy

530   • Assist in identifying who has significant cybersecurity and privacy responsibilities

531   • Provide senior leadership with regular status reports on the CPLP's goals, objectives, and
532   performance metrics

1.8.4. Managers

534   The term "Managers" includes supervisors and those who have organizational responsibilities for
535   ensuring compliance with cybersecurity and privacy learning requirements for personnel who
536   report to them. Managers should:

537   • Work with the CIO and Learning Program Managers to fulfill shared responsibilities

538   • If serving in the role of system owner or data owner, designate staff who have significant
539   cybersecurity or privacy responsibilities on their system (e.g., general support systems
540   and major applications) and ensure that users of their system are appropriately trained in
541   how to fulfill their responsibilities before being granted access to system resources.

542   • Develop individual development plans (IDPs) for personnel in roles with significant
543   cybersecurity and privacy responsibilities (these IDPs will provide guidance for assessing
544   the knowledge gaps of those with significant cybersecurity and privacy responsibilities)

545   • Promote the professional development of personnel with cybersecurity and privacy
546   responsibilities and encourage them to acquire industry-recognized certifications

547
548
- Ensure that personnel understand the specific rules of each system and application that they use

549
550
- Work to reduce errors and omissions by personnel that might be caused by a lack of awareness or training

551
552

553 **2.   The CPLP Plan and Strategy**

554 A CPLP strategic plan benefits the organization by providing an organization-wide view of the
555 current state of its cybersecurity and privacy learning, where the organization wants to or needs
556 to be, and how to address the gap between the two states (e.g., resources, staffing.) The strategic
557 plan helps the Learning Program Manager balance their daily responsibilities in ensuring that the
558 organization's personnel are ready to meet the challenges of the cybersecurity and privacy risks
559 associated with their work.

560 The Office of Management and Budget (OMB) Circular A-130 [1] establishes general policy for
561 the planning, budgeting, governance, acquisition, and management of federal information,
562 personnel, equipment, funds, IT resources, and supporting infrastructure and services. Each
563 federal agency is required to develop, maintain, and implement a comprehensive CPLP to meet
564 its mission needs. To develop a robust program that includes a variety of materials, including
565 offering learners engaging opportunities to stay current on relevant cybersecurity and privacy
566 risks to their organization, the CPLP must have an effective strategy for development,
567 implementation, and continual improvement.

568 This section discusses the steps involved in building a Strategic Plan that takes the organization's
569 objectives, unique requirements, audience types, and program scope into consideration. The
570 planning stages will also help the organization evaluate priorities, budget, resources, and
571 communication plans.

572 **2.1.   Building the Strategic Plan**

573 The CPLP must intersect with the organization's strategic plan for continual development of the
574 workforce. The owner of the CPLP should understand the structure and mission of the
575 organization to determine where the strategy originates. Some agencies are organized with a top-
576 down approach, where a headquarters function owns the mission and provides guidance on the
577 program strategy. Other organizations develop CPLPs in various business functions or combine
578 both approaches. Documenting the program and how it supports the goals of the risk
579 management strategy shows executive leadership why the program is needed. A well-developed
580 strategic plan describes how an organization's risk management and workplace learning culture
581 enable all personnel to assess risk with their every action and decision. With agencies of varying
582 sizes, a program that works for one will not necessarily work for another. Each agency must
583 identify the best program that will work for them since one size does not fit all.

584 The CPLP Strategy should always be clearly stated and will most likely be reviewed by the
585 Senior Leadership Committee and agreed upon before any funding is approved. The strategic
586 plan describes how the CPLP supports and aligns with the overall organizational risk
587 management and workforce learning strategy.

588 Key items to address in the CPLP Strategy include:

589 • Vision and mission

590 • Strategic goals and objectives

591 • Training Approaches and Action plans

592 • Tactics

593 • Metrics and reporting

594 The CPLP Strategy should also:

595 • Describe how it supports a culture of risk-based decision making and emphasize the
596 importance of transformational workforce learning, including the development of
597 knowledge, skills, and the capabilities to help workers succeed now and in the future

598 • Explain how the program will meet knowledge and skill gaps, enhance overall
599 capabilities, and support a culture of personnel engagement in their cybersecurity and
600 privacy roles

601 • Intersect with the overall mission of the organization (e.g., mission and vision statements,
602 risk tolerance, learning goals and methods, and organizational structure)

603 • Include information about organizational policies and policy owners, such as how
604 existing rules of behavior, policies, procedures, and guidance will be communicated to
605 personnel

606 • Include metrics and measures that help determine whether the program is meeting its
607 goals

608 • Include operational tactics, such as the tools, mechanisms, or methods that the program
609 owners will leverage to achieve program objectives

610 • Identify key stakeholders, leaders, and roles, many of whom will be within the offices of
611 the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Senior
612 Agency Information Security Officer (SAISO), Senior Agency Official for Privacy
613 (SAOP), or Chief Privacy Officer (CPO)

614 • Use risk assessment results and existing strategies to inform the alignment between
615 program development, learning materials, and risk management

616 ○ Gap analysis: Note that existing CPLPs may benefit from a gap analysis or
617 current program assessment to clearly distinguish between the current and target
618 states and enable the program leadership to shape their approach accordingly.

619 • Identify how the program will meet regulatory and compliance requirements to minimize
620 risks by educating personnel on their roles in the cybersecurity and privacy culture of the
621 organization

622 • Plan for and support the needs of a diverse workforce, including those with accessibility
623 requirements and those who work remotely or travel frequently

624 • Include learning methods that are experiential and atomize content (i.e., take existing
625 content and look at how it can be separated into smaller items or repurposed)

2.2. Develop CPLP Policies and Procedures

627 The CPLP policies and procedures work together to express what the organization wants to do
628 and how to do it. Policies are clear and simple statements, rules, or assertions that specify the
629 correct or expected behavior of an entity. Policies provide the guiding principles for meeting the
630 mission and conducting operations and they can help with risk-based decision-making. Policies

631 are written in broad terms and include who, what, when, and why. Procedures describe how the
632 policy will be implemented or enacted. Procedures are written to include who will do what, the
633 steps or phases for the action, defined criteria or implementation levels, and related
634 documentation.

635 For both cybersecurity and privacy business operations, policies and procedures identify
636 acceptable practices and expectations, as well as guidance for how to train personnel on those
637 requirements and expectations. It is important for the organization to have CPLP policies and
638 procedures that align with the broader policies and clearly describe the expectations for the
639 learning programs.

640 The benefits of establishing policies and procedures include:

641 • Defining clear expectations for the workplace

642 • Providing executive buy-in of the program

643 • Providing a documented management and oversight capability that can be audited

644 • Supporting cybersecurity and privacy assurance strategic goals and objectives

645 • Clearly identifying information and resources

646 • Enabling the training of personnel on their information security and privacy
647   responsibilities

648

649 **Examples of Learning Program Policy Statements:**

650 The following policy statements are not a prescriptive list of what should be included in
651 Learning Program policies. These are examples to provide context on what is important when
652 establishing, reviewing, or updating cybersecurity and privacy learning program policies. Thus,
653 the statements can include, but are not limited to:

654 • The CIO and CISO establish a cybersecurity training program for users of [organization]
655   information systems.

656 • The CPO establishes a privacy training program for users of [organization] information
657   systems that process personally identifiable information (PII).

658 • All personnel, contractors, or others who work on behalf of [organization] accessing
659   [organization] systems receive initial training and annual refresher training in
660   cybersecurity and privacy awareness and accepted cybersecurity and privacy practices.

661 • Personnel complete cybersecurity and privacy awareness training within 24 hours of
662   being granted a user account. If a user fails to meet this training requirement, user access
663   is not granted or will be suspended.

664 • All personnel, contractors, or others who work on behalf of [organization] with
665   significant security responsibilities receive specialized training prior to obtaining access
666   to the systems that process sensitive information and will be required to complete
667   refresher training each fiscal year.

668   •   All personnel, contractors, or others who work on behalf of [organization] with
669   responsibilities for processing PII receive specialized training prior to obtaining access to
670   the systems that contain PII and will be required to complete refresher training each fiscal
671   year.

672   •   User accounts and access privileges, including access to email, are disabled for
673   employees who have not completed annual refresher training unless a waiver is granted
674   by the CISO or information systems security manager (ISSM).

675   •   Privacy managers, the CISO, and ISSMs prepare and submit annual awareness and role-
676   based training plans.

677   •   Privacy managers, the CISO, and ISSMs prepare and submit cybersecurity awareness
678   reports with content, frequency, format, and distribution at the request of the CPO and
679   CIO.

680   •   The CISO reviews information security awareness and role-based training programs
681   annually.

682   Policies and procedures for cybersecurity and privacy awareness and training (learning)
683   programs can be found in NIST SP 800-53 control AT-1 [8].

2.3.   Aligning Strategies, Goals, Objectives, and Tactics

685   Organizations can utilize a variety of techniques for identifying and describing the steps needed
686   to implement a program. One method is to begin by identifying the organization's goals, the
687   objectives to meet those goals, and the operational tactics to meet those objectives. Each goal
688   should have objectives that will often include measurable targets, such as identifying who needs
689   role-based training or training a percentage of the organization by a specified date. Each program
690   objective will have tactics associated with them. Tactics are tools, methods, or mechanisms that
691   enable the program to pursue the objective identified in the plan's strategy. Ultimately, every
692   individual item in the plan – down to the most detailed tactical level – can be traced back to
693   where it originates in the overall strategy. It is important that every activity support the overall
694   CPLP strategy. Managing the steps to implement CPLPs and ensure that the program meets
695   organizational learning needs requires discipline on the part of the team.

696   **Table 1** outlines a model for the strategy that includes goals, objectives, and tactics.

697   **Table 1.** Elements of a CPLP strategy

Step	Description
Strategy Plan	Learning Program Managers meet to set or reset priorities and develop the CPLP Strategic Plan.
Strategic Goals	Define distinct elements of the Strategic Plan around which to organize the program. Examples of these include goals such as decreasing susceptibility to social engineering attacks, identifying when to apply privacy risk management measures, increasing the adoption of multi-factor authentication, or including scenario-based training activities.

Step	Description
Objectives	Based on the strategic goals, develop objectives that include distinct measurable outcomes and the types of metrics associated with the program element.
Tactic	Based on the objectives, develop tactics (i.e., the mechanism that the CPLPs will use to achieve a program objective in part or in full). Examples include a phishing exercise to promote awareness of social engineering attacks, enterprise-wide newsletters or other announcement mediums, webinars on multi-factor authentication basics and procedures, or brainstorming sessions with subject matter experts on scenario development.

698

699   The following two example scenarios demonstrate each of the implementation steps.

700   **Scenario 1: Protecting Sensitive Printed PII**

701   A physical security review of an area in the organization where sensitive personally identifiable
702   information (PII) is routinely handled by many employees finds that basic steps are not being
703   taken to maintain a "clean desk." Privacy policy requires files that contain sensitive PII to be
704   kept in folders in locked cabinets. During the review, printed files containing sensitive PII were
705   located in paper stacks and in folders loosely placed on the top of the desks.

706   The organizational strategy is to improve the handling of printed sensitive PII and ensure that
707   personnel follow the protection requirements. The Learning Program Manager determines that a
708   fresh, eye-catching awareness product may encourage better employee adherence to policy and
709   reduce this risk.

710   An executive offers available funding dedicated to producing printed materials. The Learning
711   Program Manager may be able to utilize that funding to print "Keep It Clean" stickers to attach
712   to work folders and provide a case of such folders to each member of the workforce in the area
713   that handles sensitive PII materials.

714   In this example, the privacy Learning Program Manager participated in the continual monitoring
715   of the workplace and risks, coordinated the budget, planned the printing of the stickers, and
716   worked with management to deliver the materials. Because this is a one-time issue, the planning
717   steps were streamlined under the existing program.

718   *Strategy* – Meet privacy compliance requirements

719   *Strategic Goal* – Support the organization's Privacy Program

720   *Objective* – Ensure that all employees who handle sensitive PII are trained and aware of
721   privacy responsibilities

722   *Tactic* – Provide "Keep It Clean" stickers on folders to each employee in areas of the
723   organization where sensitive PII is processed

724

725   **Scenario 2: Developing new regulatory-required training program**

726   A new regulation requires all cybersecurity professionals to implement a specific procedure in
727   their daily routines.

728 The cybersecurity Learning Program Manager works with the cybersecurity policy owners to
729 understand and interpret the guidance. Once completed, they define a strategy with goals and
730 objectives and identify a set of program tactics that would deliver new training to all members of
731 the workforce and meet the new requirements with specific new procedures. The cybersecurity
732 Learning Program Manager decides to work with organizational training staff to create an online
733 experience, which would also enable remote workers to participate fully.

734 As the course is being completed, the cybersecurity Learning Program Manager works with
735 organizational leaders and management to identify expected measures of completion and success
736 and to ensure that all necessary members of the workforce are identified and trained. As an
737 element of continuous monitoring, the cybersecurity Learning Program Manager works with the
738 learning office and leadership to test the completion and success of the training.

739 *Strategy* – Meet new regulatory requirements

740 *Strategic Goal* – Train cybersecurity professionals

741 *Strategic Goal* – Build and deliver online training program

742 *Objective* – Launch new online training program that will enable all employees to meet
743 the new procedure training objectives, even from remote work locations

744 *Tactic* – Work with management to schedule the training and ensure 100 % compliance
745 in training

746 *Tactic* – Enable a continuous monitoring program to test completion rates and provide
747 daily tracking to managers

748 ## 2.4. Determining CPLP Measurements and Metrics

749 Program measurements and metrics are essential to show the effectiveness and impact of the
750 program, understand where changes are required for success, and meet continued budgetary and
751 resource requirements. There may be regulations that apply.

752 Metrics should determine what should be measured and why. While laws, regulations, and
753 policies often set specific measurable requirements, CPLP metrics should go beyond simply
754 achieving compliance and serve to help measure the CPLP's impact on workforce attitude and
755 behavioral changes. The metrics should be tied directly to the goals of the program. The
756 Learning Program Managers should identify how the metrics will be collected, how frequently,
757 who should have access to them or receive reports that include information about them, and how
758 they will be shared.

759 Policies and regulations need to be considered, since they often set specific guidelines on what
760 information to gather. CPLPs should be prepared to answer some common questions, such as:

761 • What policies apply to our organization?

762 • How often is reporting required?

763 • What data is required in the report?

764 • What data are we required to maintain for potential audits?

765 Learning Program Managers should build programs with efficient data gathering techniques to
766 provide effective reporting information. This will likely include collecting PII on employees that
767 may carry a heightened sensitivity due to context (e.g., training records are often part of
768 employment or contract records and can be tied to performance evaluations or result in
769 consequences for failing to take required training). Learning Program Managers must identify
770 and manage the cybersecurity and privacy risks associated with processing learning data,
771 including risks associated with learning management systems and reporting practices.

772 Developing a CPLP metrics plan can be one of the most important yet most challenging parts of
773 the CPLP effort. An effective set of measurements can help the program get support from the
774 organization, increase funding, reveal impact on the cybersecurity risk management program,
775 and demonstrate returns on investment. In recent research efforts by NIST, participants reported
776 [10] that despite best intentions, their organizations often used a limited number of metrics that
777 did not provide a complete view of program effectiveness. NIST SP 800-55 *Performance*
778 *Measurement Guide for Information Security* provides guidance on the selection, development,
779 and aggregation of information security measures and developing an information security
780 measurement program.[9]

781 **Examples of Quantitative Learning Program Data:**

782 • Cybersecurity incident data, limited to employee-generated incidents or topics that
783 can be mitigated or addressed in the learning programs

784 • Metrics on incident reporting, demonstrating employee ability to recognize and report
785 potential cybersecurity events

786 • Phishing or other simulated attack responses

787 • Longitudinal data that depicts program impact over time

788 • Employee testing data before the learning program, immediately after the learning
789 program, and three months after attending the course to assess knowledge retention

790 • Performance data by department, including technical performance measures

791 • Training attendance, performance assessments, and completion rates

792 • Closed-ended (quantitative) employee survey feedback

793 • Cost of development and delivery invested per participant

794 • Frequency of updating the training material may be used to evaluate relevancy

795 • Extent of cybersecurity or privacy events, such as reduced downtime or outages due
796 to events (these may be indicators for role-based training)

797 • Ability to recognize and report privacy information disclosures or misuse

798 • Changes following technical training may also provide measurements, such as
799 reduction of accounts with privileged access, identification of high value assets, new
800 network segmentation, or additional controls written in acquisition and budget
801 documentation

---

[9] NIST SP 800-55 is currently in development; NIST plans to issue a draft for public comment by Q1 FY2024.

802

Examples of Qualitative Learning Program Data:

804   • Presenter and program feedback

805   • Open-ended survey fields

806   • Detailed reports from participants

807   • Focus groups

808   • Observations of learning program participants

809   • Suggestion box submissions

810   **2.5. Learning Program Participants**

SIGNIFICANT CYBERSECURITY OR PRIVACY RESPONSIBILITIES
Determined by individual development plan, manager, or work role

PRIVILEGED USER
Additional cybersecurity and privacy training

ALL USERS
Onboarding training, acceptable use policies, annual learning program, or awareness campaigns
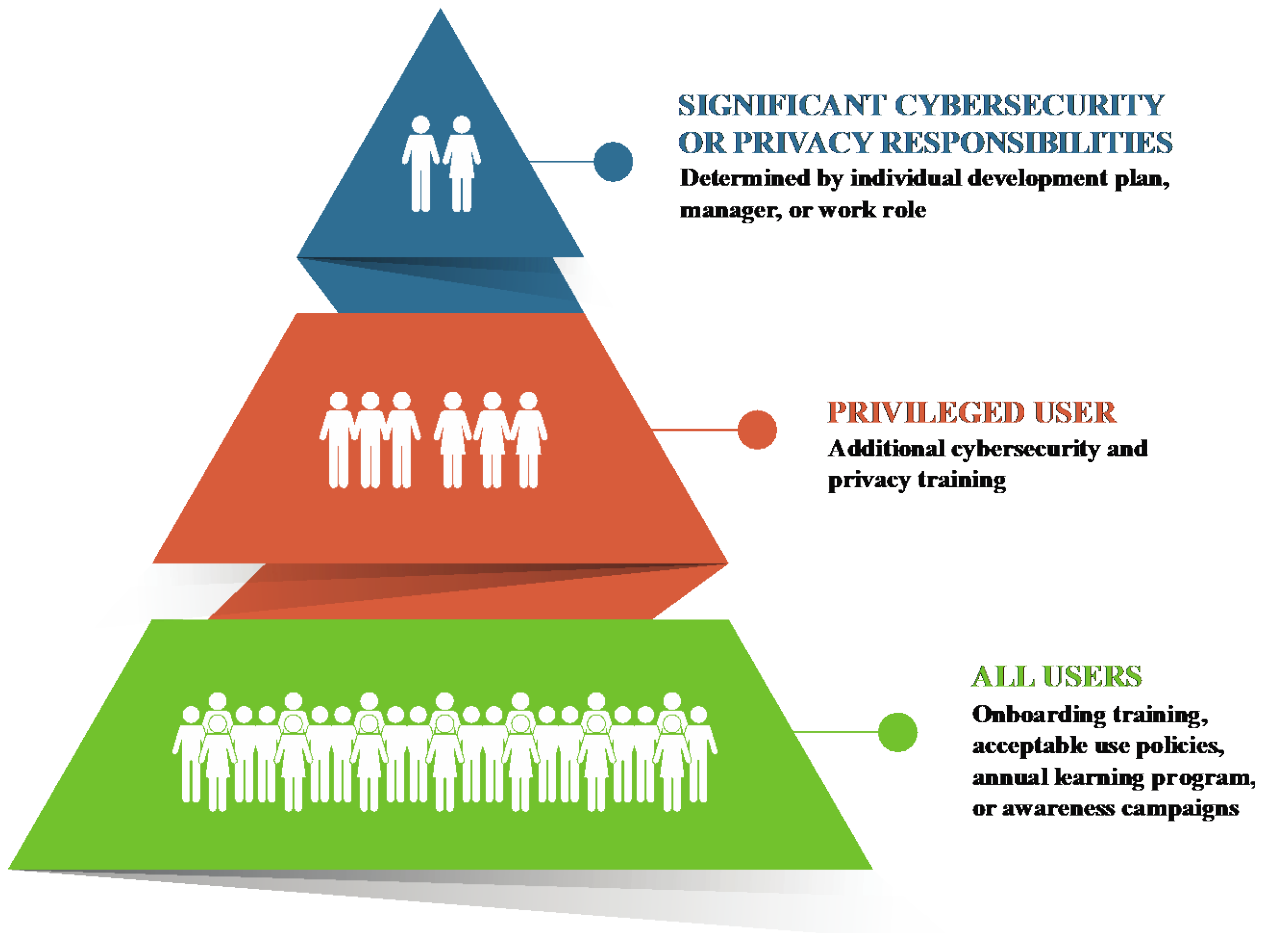
811

812   **Fig. 4.** CPLP Learning Program participants

2.5.1. All Users

In a typical scenario, all of the organization's personnel (i.e., the general workforce, including contractors) will participate in the CPLP, agree to abide by the Acceptable Use Policy or Standards of Behavior, complete the annual Learning Program training, and attend, complete, view, and receive the other various ongoing program elements.

In NIST SP 800-53 [8], All User training is referred to in the Awareness and Training control (AT-2) as cybersecurity and privacy "literacy" training. As part of or after completing the annual training, users will sign a Rules of Behavior that defines the behaviors required to gain and keep system access. NIST SP 800-53 additionally indicates that the training will also need to be updated for any system changes or following any organization-defined events:

"Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines."

All users in the workforce (previously referred to as "system users" and "general users") are critical to reducing unintentional errors and vulnerabilities. The organization's personnel may include employees, contractors, foreign or domestic guest researchers, visitors, guests, other agency personnel, and other collaborators or associates who require access. All users must:

- Understand and comply with the organization's cybersecurity, physical security, and privacy policies and procedures

- Understand and accept the rules of behavior for the systems and applications to which they have access

- Work with management to meet training needs

- Be aware of actions they can take to better protect their organization's information and environment

Examples of topics that the CPLP may address include understanding how cybersecurity and privacy activities support the organization's mission and business objectives; using proper passwords; backing up data; using proper antivirus protection; reporting any suspected incidents or violations of cybersecurity and privacy policies; following the rules established to avoid social engineering attacks (e.g., ransomware and phishing) and to deter the spread of spam, viruses, and worms; identifying and addressing privacy risks during information processing; and knowing where to find the organization's cybersecurity and privacy resources and points of contact.

2.5.2. Privileged Users

Privileged users are trusted with additional access or responsibilities to perform cybersecurity- and privacy-related functions that ordinary users are not authorized to perform. Due to the specialized functions that privileged users typically perform and their ability to access critical resources of the organization, privileged users require additional training to ensure that they understand their account privileges and do not accidently cause or exploit vulnerabilities.

854   Examples of such responsibilities include configuring network management and granting system
855   access (e.g., system administration privileges). For each type of privileged user, the Learning
856   Program Manager must coordinate training with their manager or supervisor, human capital
857   officer, and the training managers to ensure that training is delivered and kept current.

858   2.5.3. Staff with Significant Cybersecurity or Privacy Responsibilities

859   Personnel with significant cybersecurity or privacy responsibilities and some of the privileged
860   users will be required to have training due to the nature of their role within the organization.
861   There are circumstances in which personnel have rights or access to sensitive or critical systems
862   and, therefore, will require additional training. The permitted personnel will have additional
863   access that can be rescinded when their work role changes. Examples of such environments
864   include acquisitions, financial management, healthcare, human resources, and web publishing.

865   NIST SP 800-53, the Role-Based Training control (AT-3) provides a definition for the training
866   required:

867   Comprehensive role-based training addresses management, operational,
868   and technical roles and responsibilities covering physical, personnel, and
869   technical controls. Role-based training also includes policies, procedures,
870   tools, methods, and artifacts for the security and privacy roles defined.
871   Organizations provide the training necessary for individuals to fulfill
872   their responsibilities related to operations and supply chain risk
873   management within the context of organizational security and privacy
874   programs. Role-based training also applies to contractors who provide
875   services to federal agencies.

876   This training is typically associated with job duties determined by organizational leaders, such as
877   the agency's CIO, CPO, or CISO and the employee's manager or supervisor, and is typically
878   documented in the employee's performance plan. Personnel in these work roles may require
879   professional development to maintain their professional status or memberships, such as annual or
880   regular professional certifications or courses. Examples of typical role-based training recipients
881   include the CISO, privacy officers, cybersecurity managers, cybersecurity and privacy analysts,
882   and incident responders. References for cybersecurity work roles or competency areas are
883   explored in NIST SP 800-181r1 [3], which describes the knowledge, skills, and tasks associated
884   with cybersecurity-related work.

885   2.5.4. Determining Who Has Significant Cybersecurity and Privacy
886   Responsibilities

887   FISMA [9] requires personnel with significant cybersecurity and privacy responsibilities to
888   receive role-based training. Additional guidance can be found in NIST SP 800-37 [7], NIST SP
889   800-53 [8], and NIST SP 800-181r1 [3]. In combination, these documents assist with the
890   identification of roles and functions in the cybersecurity workforce that require role-based
891   training. As this document covers the concepts of managing a Learning Program for privacy as
892   well, consider how to extend the same concepts to help privacy professionals meet their own
893   role-based or significant privacy training needs.

894   Determining who in the organization will participate in role-based training is a multi-step
895   process that begins with defining the significant cybersecurity and privacy work roles in the
896   organization and identifying the staff who are aligned with the designated work role. Often, the
897   determination begins with senior leadership with direction from the office of the CIO, CISO, or
898   CPO and in partnership with the Human Resources department. The Learning Program Manager
899   should participate closely in this effort to identify those on their team who have significant
900   cybersecurity and privacy responsibilities and need additional training.

901   The work roles should also be included in position descriptions, hierarchy charts, and
902   responsibilities to show how the work required to achieve a particular objective has been
903   identified. Individuals may assume additional work roles based on their particular skills,
904   organization policies regarding cross-training, and organizational staffing levels. NIST SP 800-
905   181r1 [3] identifies work roles for cybersecurity and is a detailed lexicon for understanding the
906   related knowledge and skills typical for such roles.

2.6.   Determining Scope and Complexity

908   When building any CPLP, the ultimate goal is to reduce risks to the organization, not simply
909   achieve compliance. The material should be appropriate in scope and complexity for the
910   participant, so it is necessary for the Learning Program Managers to consider the different types
911   of workforce participants who will participate in the program. The program material should also
912   contain the right level of complexity and technical knowledge for the audience's learning
913   objectives and fulfill their training and awareness needs. This requires coordination with Human
914   Resources and the Chief Learning Officers (CLO), or equivalent, in the organization to recognize
915   the roles and responsibilities of individuals in the organization.

916   Individuals who receive the training will appreciate the effort made to ensure that they
917   understand the material in a manner appropriate to their learning needs and the nature of the
918   work that they do. The complexity of the material must be determined before development
919   begins and commensurate with the role of the person who will undergo the learning effort.
920   Material should be developed based on two important criteria: 1) the target attendee's role, and
921   2) the cybersecurity and privacy responsibilities required for that role.

2.7.   The CPLP Elements

923   A typical CPLP includes a variety of learning program elements that are delivered to diverse
924   audiences through a variety of platforms and methods. The Learning Program Manager will
925   work to identify the necessary and most effective types of program elements for each audience
926   type, per learning goal, and adjust their selections to match their available budget and schedule
927   considerations.

928   The typical CPLP elements are:

929   • Awareness Activities

930   • Practical Exercises

931   • Training

932 When the average person thinks of a CPLP, they likely think of the annual training event
933 delivered to All Users. These might be informal department programs, an all-hands presentation
934 delivered in an auditorium, or an online course. Other learning program elements are targeted for
935 those with significant cybersecurity responsibilities, including privileged account holders. A
936 CPLP program will consist of the mandatory elements (required by policy and learning
937 objectives for all CPLP learning participants) and the many other activities implemented
938 throughout the life cycle to reinforce these messages.
939
940 The learning goals for these events are to ensure that personnel are aware of their roles and
941 responsibilities for protecting assets and are able to take appropriate action against a variety of
942 cybersecurity and privacy risks.

2.7.1. Awareness Activities

944 Cybersecurity and privacy awareness learning activities are implemented throughout the year to
945 remind users about a wide variety of risks. Awareness activities should be conducted on an
946 ongoing basis to ensure that employees are aware of their roles within the organization and the
947 appropriate steps they must take for the protection of information, assets and individuals'
948 privacy. Activities can be campaign-oriented or ad hoc based on the subject matter, threats, or
949 vulnerabilities or during seasonal events.

950 Examples of awareness activities that are appropriate for All Users include:

951 • Learning program messages on logon screens, organization screen savers, and email
952 signature blocks

953 • Employee newsletters with cybersecurity and privacy articles

954 • Posters (physical or digital) with cybersecurity and privacy tips

955 • A Cybersecurity Awareness Month or Privacy Week activity fair

956 • Cybersecurity and privacy reminders and tips on employee materials (e.g., pens,
957 notepads, etc.)

958 • Periodic or as-needed email messages that provide timely tips, or that are sent in response
959 to a cybersecurity or privacy event or issue.

960 Consider that each October is designated as "Cybersecurity Awareness Month" and is, therefore,
961 a popular month for scheduling various learning activities. Each January, there is a "Data Privacy
962 Awareness Week," and it is also a popular time to schedule privacy protection learning events.
963 Leveraging annual themes and available resources can enhance these special events.

2.7.2. Practical Exercises

965 Practical exercises or experiential learning activities are specific learning scenarios that simulate
966 events and incidents. The practical exercises can include phishing exercises and other social
967 engineering campaigns, learning games, quizzes on identifying and processing PII, tabletop
968 exercises, hands-on virtual lab exercises, contingency plan and disaster recovery scenarios, and
969 attack or defend scenarios conducted in cyber ranges.

970   An organization-wide All-User phishing exercise is a typical type of practical exercise. In a
971   phishing exercise, a "tricky" email is sent to users to see whether the user can spot a phishing
972   attempt or if they can be tricked into clicking on a link to a malicious website or opening an
973   infected attachment. Since phishing emails can target specific roles in the organization, such as
974   leadership or known administrators, the phishing exercises can also target specific roles.
975   Phishing exercises offer opportunities to collect metrics and measurements, which are usually
976   referred to as click-through or reported measurements. These types of measurements indicate
977   whether the user reported the email as a phishing attempt or whether they clicked on a link or
978   opened an attachment. Some organizations include "report phishing" capabilities on their email
979   platform (e.g., a button on the platform's menu) to encourage best practices. It can be important
980   to consider the context of the employee's work when creating or deploying a phishing test.[10]

981   Be sure to include the organization's legal team in the design review of planned phishing
982   exercises to avoid negative impacts, such as using legitimate brands or naming federal
983   organizations in the phishing "bait," which could result in emails or calls to those entities. In
984   addition, since employees may not like being tricked, it is important to tell employees that the
985   organization is conducting phishing exercises on a random basis and that the results will be used
986   to guide future learning activities. These activities should not be punitive, nor should any
987   employee be called out for their response. When viewed as learning opportunities, the phishing
988   exercises can provide important data on vulnerabilities and which employees may need
989   additional learning support.

990   Other practical exercises may be better suited for those with significant cybersecurity or privacy
991   responsibilities (e.g., role-based training) or, if well-designed, could apply to any user group.
992   These exercises might include table-top exercises and contingency plan scenarios. Additional
993   examples may be found in the 2006 NIST SP 800-84, "*Guide to Test, Training, and Exercise*
994   *Programs for IT Plans and Capabilities*"[4].

995   ### 2.7.3. Training

996   Training is a broad term that includes the Learning Program content designed to increase or
997   improve job-related knowledge and skills. Some of the techniques that an organization can
998   employ include:

999   • **Synchronous training:** Instructors and students participate together, whether in a virtual
1000   or a physical classroom-based learning environment.

1001   • **Asynchronous training:** The learner is able to access material individually and on-
1002   demand. This is sometimes called "self-paced" because the learner accesses content
1003   based on their schedule.

1004   • **Virtual led:** Instruction occurs in a virtual or simulated environment and is presented or
1005   facilitated by an instructor in real time.

1006   • **Cyber range:** Instruction takes place in a safe web-based practice environment (i.e.,
1007   sandbox) and delivers hands-on realistic training, scenarios, challenges, and exercises.

---

[10] The NIST Phish Scale considers employee context in its method for determining the difficulty of a simulated phishing email.
https://www.nist.gov/news-events/news/2020/09/phish-scale-nist-developed-method-helps-it-staff-see-why-users-click

1008   •   **Podcasts:** Learning is asynchronous, self-paced, and typically audio based.

1009   •   **Animations:** Animations can visually represent a process, system, or complex
1010   cybersecurity or privacy concept.

1011   •   **Demonstration:** The instructor provides the learner with the step-by-step actions of a
1012   process or activity. This can be delivered in-person, recorded, or via other methods.

1013   •   **Scenario-based exercise:** The facilitator leads discussions on topical, situation-driven
1014   scenarios that may be customized to the organization or to a specific department. These
1015   are also referred to as "table-top" exercises.

1016   •   **Self-paced online training:** This asynchronous technique is currently popular for
1017   distributed environments. Attendees of a web-based session can study independently and
1018   learn at their own pace. Testing and accountability features can gauge performance. Web-
1019   based training can include video, audio, and interactive techniques, such as drag-and-drop
1020   or fill-in-the-blank exam responses.

1021   •   **Onsite instructor-led training:** This is one of the oldest and most popular techniques for
1022   delivering training material to an audience. The biggest advantage of the technique is the
1023   interactive nature of the instruction. It can also include peer presentations and mentoring.

1024 Blending various training delivery techniques can be an effective way to present material and
1025 hold an audience's attention. For example, showing videos during an instructor-led session
1026 allows the audience to focus on a different source of information. The video can also reinforce
1027 what the instructor has been presenting.

2.8.   Establishing the CPLP Plan Priorities

1028

1029 There are many elements to consider when entering into the planning phase of the CPLP life
1030 cycle. A leading consideration is to evaluate the organization's critical risk factors to determine
1031 the learning priorities. If a phased approach is necessary, such as due to budget constraints or
1032 resource availability, some factors to consider are:

1033   •   **Role and organizational impact** – It is very common to address priority in terms of
1034   organizational role and risk. Broad-based awareness initiatives that address the
1035   enterprise-wide mandate may receive high priority because the rules of good
1036   cybersecurity and privacy practices can be delivered to the workforce quickly. It is also
1037   common to look at *high trust/high impact* positions (see earlier discussions about
1038   cybersecurity and privacy specialist roles) and ensure that they receive high priority in
1039   the rollout strategy. These types of positions are typically commensurate with the type of
1040   access (and to what systems) these users possess or specialized requirements assigned to
1041   their roles and job duties.. In addition, the protection of high value or critical assets or the
1042   deployment of privacy-sensitive products or services can also drive priorities.

1043   •   **State of current compliance** – This involves looking at major gaps in the CPLP (e.g.,
1044   gap analysis) and targeting deficient areas for attention.

1045   •   **Availability of materials and resources** – Determine whether appropriate learning
1046   material and necessary resources are readily available for the program element.
1047   Repurpose and utilize existing materials in new ways, when possible.

1048   **2.9.   Developing the CPLP Plan**

1049   The Learning Program plan refers to the working documents that contain elements that support
1050   the strategy for each activity or campaign. A Learning Program plan, such as what might be
1051   created to build an awareness campaign or privileged account holder training, is similar to a
1052   project plan. The purpose of creating Learning Program plans is to guide the delivery of the
1053   program elements. This document defines the program element with sufficient detail to inform
1054   key stakeholders and contributors to perform their roles successfully. Many organizations utilize
1055   standard program plan templates that provide baselines for organizational expectations.

1056   The exact level of detail within the plan will vary, depending on organizational and program
1057   requirements and resources. As the program matures, the Learning Program Manager should
1058   conduct recurring reviews (i.e., at least annually) of the plan, along with the stakeholders and
1059   individuals who will support and manage the program.

1060   **2.10.   CPLP Resources**

1061   An important element of developing the CPLP Strategy is to determine what currently exists
1062   within the organization and what resources are dedicated to the existing programs. If the
1063   Learning Program does not exist or requires significant redesign or updates, refer to the Program
1064   Strategy process outlined in Section 2.1 to review the most important program elements for
1065   inclusion. Resources are typically defined as any asset that is required to meet the goals and
1066   objectives, such as people, materials, equipment, and technology. An important consideration in
1067   obtaining resources is establishing a CPLP budget.

1068   **2.10.1.   Establishing a CPLP Budget**

1069   Once the CPLP strategy has been approved by the senior leadership (identified in Section 1.10.2)
1070   and the priorities have been established, funding requirements must be added to the plan. A
1071   determination must be made regarding the extent of funding support to be allocated based on the
1072   strategic goals. Senior leadership should help the Learning Program Manager understand or
1073   establish their budget. While each program will have different funding needs, some typical costs
1074   include:

1075   • Training personnel, such as program managers, instructional designers, instructors,
1076   graphic artists, web developers, and programmers

1077   • Classroom space and materials, such as whiteboards, markers, erasers, flip charts, note
1078   pads, pens, pencils, and name cards

1079   • Printed program materials, handouts, and certificates or electronic distribution that may
1080   require web-based platforms

1081   • Online (virtual) space to distribute materials, including synchronous activities such as
1082   webinars and asynchronous activities such as job aids, recorded sessions, and web-based
1083   content

1084   • Learning Management Systems for content delivery, participant registration, and course
1085   completion records

1086   • Licenses (per-seat) for learning platform or content

1087   • Awareness materials, such as posters, notepads, and themed items for awareness
1088   activities

1089   • Professional services for curriculum design and development and the presentation of
1090   content, as well as any additional associated costs

1091 There are strategic and cost-benefit decisions that the organization must make to ensure that the
1092 CPLP is adequately funded. Some materials may be available from other federal agencies,
1093 partner organizations, or online vendor resources. Some materials may already exist in-house and
1094 should be inventoried and evaluated to determine whether they are current and meet the existing
1095 training goals. The implementation timeline will help indicate when additional funding may be
1096 required to support tools, major curriculum and content deliverables, new staffing requirements,
1097 and other learning program elements and activities.

1098

The following are example questions that can help guide development of budget requirements:
  • What mission and business needs will be influenced or impacted?
  • Are there regulations, legislative requirements, or other internal or external
    requirements that would influence the decision?
  • What shared federal or other external resources can be leveraged?
  • What internal resources can be leveraged? This can include existing content and
    delivery mediums.
  • Is it more cost-effective to develop the material in-house versus outsourcing?
  • Is the learning requirement specific to the organization or the system? This would
    include information such as specific policies, procedures, or rules of behavior.
  • When must the learning material be ready? Are there critical schedules that need to be
    met? Would outsourcing allow for delivery schedules to be met?
  • How many people need to be trained?
  • How often will the material need to be updated?
  • What delivery mediums will be required, and what are the associated costs?
  • Are there in-house resources to do the job?
  • Does the organization have the subject-matter expertise to provide content for the
    training?
  • Are resources available to effectively manage and monitor contractor activity during
    acquisitions?
  • Does the course sensitivity preclude the use of a contractor?

1099

1100 The Learning Program Manager must work with senior leadership to advocate for the Program
1101 against competing priorities and develop a strategy to address any shortfall in funding that may
1102 impact the organization's ability to meet its learning goals. This may mean adjusting the learning
1103 strategy to be more in line with the available budget, advocating for additional funding, or
1104 reallocating current resources. It may also mean that the program plan needs to be phased in over
1105 some predefined time period as funding becomes available.

1106 **2.10.2.   CPLP Staff and Locations**

1107 Those who have managed federal CPLPs report that training the workforce requires a
1108 combination of technical knowledge and professional attributes, such as communication,
1109 creativity, and interpersonal skills [11]. If the organization does not have the budget for CPLP
1110 course developers, determine what other agencies or organizations of similar size have done for
1111 their own needs. Some organizations may have in-house instructional designers, curriculum
1112 developers, instructors, web developers, communication experts, and graphic designers. Other
1113 organizations may need to include these professional costs in the budget for a new project.
1114 Identify qualified contractors to use or external courses that the organization can purchase.

1115 Different information requires different methods of delivery. Some program elements will be
1116 appropriate to deliver via online learning, while others will necessitate both instructors and
1117 physical classroom locations. Determining these requirements up front will allow for appropriate
1118 resource allocation (e.g., rooms to be reserved, computers and projectors secured, etc.). Even
1119 posters and flyers require space considerations, as they will need to be displayed in a sufficiently
1120 prominent area to have a learning impact on the personnel.

1121 **2.11. Communicating the Strategic Plan and Program Performance**

1122 One of the most important aspects of executing the CPLP Strategic Plan is collaborating with the
1123 learning team, key stakeholders, senior leadership, and personnel. Involving stakeholders and
1124 employees during the planning process can lead to greater success as the program begins and as
1125 each program element is implemented. Determining what to communicate should focus on:

1126 • How the CPLP helps meet organizational and learning goals

1127 • How the CPLP elements will impact personnel

1128 • Engaging with stakeholders to determine concerns or conflicts in advance

1129 • Soliciting feedback to identify gaps or missing elements in the plan

1130 Getting early and continual buy-in for the strategic plan is important to keep the momentum for
1131 the CPLP strong and to inspire engagement and satisfaction with the plan. A solid
1132 communication strategy will address those needs. Consider whether the organization has a
1133 centralized communications department or whether communications decisions will be made at
1134 the business unit level. Then develop a communications plan (or incorporate these elements into
1135 an existing communications plan) to share information about the new or updated CPLP. Keep it
1136 simple and tailored to internal stakeholders. The Learning Program Manager may choose to
1137 create a custom version of the strategic plan that includes different information for different
1138 audiences.

1139 Some important elements to share include information about what the CPLP is and who manages
1140 it. Funding issues and gaps may also need to be identified and addressed. For example, agency
1141 leaders and managers need to know whether the cost to implement the CPLP activities will be
1142 funded by the CIO, CISO, CLO, or another program budget or whether their budgets will be
1143 impacted to cover a portion of the expense. In addition, schedules and completion requirements
1144 must be communicated.

1145   Elements of the CPLP communications should include:

1146   •   An overview of the CPLP strategy and ownership

1147   •   Goals, objectives, and assessment processes

1148   •   A list of key roles and their respective responsibilities, including:

1149   o   Senior leadership and executives

1150   o   Managers and supervisors

1151   o   Human Resources (HR), Office of the Chief Human Capital Officer (OCHCO),
1152   and labor relations

1153   o   Office of the Chief Financial Officer (CFO) or budget analyst

1154   o   Chief Learning Officer (CLO) (agency or organization level)

1155   o   Learning Program Managers and team members

1156   o   Subject-matter experts

1157   •   Budget overview

1158   •   Key deliverables and high-level schedule

1159   •   Measurements and metrics

1160   •   Reporting methods and frequency

1161   It is essential for everyone involved in the implementation of the program to understand their
1162   roles and responsibilities. Most organizations may find it helpful to tailor their messaging based
1163   on the audience. A few examples of audiences and their roles include:

1164   •   **Senior leadership and executives** (e.g., CIO, CISO, SAISO, SAOP, and CPO) –
1165   Communications may include a high-level summary of the CPLP strategic plan,
1166   including the goals for and phases of the yearlong program. The senior leadership needs a
1167   good sense of the overall program so that they can support the allocation of budget and
1168   personnel. Ensure that senior leaders are provided with appropriate messaging so that
1169   they can avoid harmful language, such as "users are the weakest link."

1170   •   **Managers and supervisors** – Communications should emphasize the benefit of building
1171   a positive cybersecurity and privacy culture and help the manager or supervisor recognize
1172   their crucial role in supporting that culture. An objective for their buy-in is to encourage
1173   positive associations with allocating time for employee learning.

1174   •   **Human Resources, human capital officers, and labor relations officers** – Those
1175   involved in Human Resources or human capital are responsible for any required
1176   communications regarding the implementation of CPLP requirements into the onboarding
1177   and training of union members throughout the year. If appropriate, the labor relations
1178   officers will also be key stakeholders in assisting with any updates to the plan and
1179   receiving reports on learning outcomes and other metrics for their union-represented
1180   personnel. Human capital is also a crucial stakeholder to provide input about personnel
1181   disciplinary actions and to initiate labor relations and union negotiations with regard to
1182   the mandatory training or learning activities outlined in the agency process.

1183 • **Chief Financial Officer** – The Office of the Chief Financial Officer (or the organization
1184 or agency equivalent senior financial officer) is responsible for approving the CPLP and
1185 dispensing funding to the Learning Program Managers and must, therefore, be kept
1186 informed about program implementation and measurements.

1187 • **Chief Learning Officer** – The Chief Learning Officer is responsible for learning in the
1188 organization and is an important ally for the CPLP. The CLO may provide the learning
1189 infrastructure, such as the Learning Management System (LMS) or other distribution
1190 platforms.

1191 • **Personnel** – Create a communications strategy that allows for direct email messages to
1192 personnel, as well as a distributed system to their managers and supervisors. When
1193 creating communications materials about the CPLP for individual contributors, such as
1194 email blasts or the materials in the new hire orientation packages, focus efforts on
1195 enabling the individual contributor to see their part in the overall CPLP. It should include
1196 a schedule to ensure that users are notified in sufficient time before they are required to
1197 complete the learning activity.

1198

1199

3.   Analysis and Design of the CPLP

To create a highly effective CPLP, the Learning Program Manager will dedicate time and resources to analyzing and designing the program. During the analysis phase, they identify their organizational and learning needs or gaps. The gaps are reviewed to determine which audiences will need training and and their existing levels of knowledge and skill(s). It may be necessary to evaluate various workroles for learning gaps so that relevant learning programs can be customized and created based on the specific learning needs for the workrole. During the design phase, the gaps are translated into learning objectives, which are the focus of the learning material. Tying the learning objectives to identified knowledge and skill gaps ensures that the end result is relevant and will succeed in closing the identified learning needs.

3.1.   Analysis Phase

The analysis phase is the process during which the Learning Program Manager determines the organization's learning and performance needs. In this context, the needs, which are also called gaps, are the difference between the current learning goals (or activities) and the desired state. To determine their learning needs, organizations may conduct a formal or informal needs assessment (also referred to as a needs analysis). The primary benefit of the analysis phase is to identify both learning needs for the organization and the learning audience. Additional benefits include having information that clearly defines the learning needs, support for resources and the prioritization of resources, and the alignment of learning goals to organizational mission goals.

In the beginning of the analysis phase, it may be helpful to identify the primary members of the analysis team, including several additional constituent groups. This may include the following:

- **Executive management** – These organizational leaders understand the relevant regulations, directives, laws, operational changes, or other requirements that form the basis for the CPLP. It is important for the leadership to provide input to the organizational learning needs since they set the expectations for the program and the personnel. A key role for the Learning Manager in driving learning programs is to continually advocate for the program. The Learning Manager will make the case for why analysis is important and how an effective CPLP is part of effective risk management. Additionally, an effective and well-designed CPLP supports the development of an organizational culture focused on cybersecurity and privacy protections.

- **Cybersecurity and privacy personnel**– These individuals act as subject-matter experts and consultants for the organization. They identify and help document the knowledge and skills needed to perform work roles.

- **System owners and Program Managers** – These individuals will have information and responsibilities for the particular system in use by the organization. For example, the owner of the financial system will recognize the impact of a goal on the personnel tasked with operating that system.

- **Learning Program participants** - Representatives from the employee base and from different cybersecurity and privacy work roles can lend their voice and input into the requirements gathering and analysis process.

1240 ### 3.1.1. The Importance of the Analysis Phase

1241 There are many reasons why the analysis phase is rushed or skipped entirely. For example,
1242 organizations may think it will take too much time, personnel may be unavailable, or the
1243 necessary funding may be lacking. Most often, organizations believe they already know what
1244 they need. However, critical problems can arise by skipping the analysis phase, such as:

1245 • Wasted spending when learning materials are developed that do not meet the required
1246   knowledge or skill gaps

1247 • Misunderstanding the knowledge and skills gaps of the employee participants, which may
1248   require personnel, technology, or other resources to remedy

1249 • Using training to solve an issue that is not a knowledge or skill gap. For example, an
1250   employee is unable to perform "additional as assigned" duties. Conducting an analysis
1251   will help to determine if it is a systematic or structural gap instead of a learning gap.

1252 • Providing the right personnel with the wrong information, such as giving privileged users
1253   only basic training rather than information specific to their additional rights

1254 • Providing the wrong personnel with the right information, such as giving privileged user
1255   training to general users

1256 • Providing the right information through an ineffective medium or providing the wrong
1257   information through a flashy medium

1258 • Repeating the same learning material even if previous efforts have failed

1259 It may be tempting or even overwhelming to think about setting aside time to analyze the
1260 organization's needs. Even if the only option is to conduct an informal discussion and review
1261 with a few individuals, it is still important to have the conversation and document what is
1262 needed. The analysis phase establishes a clear vision for the next steps of the Learning Program's
1263 development.

1264 ### 3.1.2. The Steps of the Analysis Phase

1265 While there are many ways that a Learning Program Manager can evaluate the learning needs of
1266 the organization, the process for identifying Learning Program needs from a strategic point of
1267 view tends to be a repeatable process, regardless of the specific learning goal or audience. The
1268 steps are:

1269 1. Identify the learning needs

1270 2. Determine the learning audience

1271 3. Identify the knowledge or skills relevant to the goals per audience

1272 4. Assess the audience's current knowledge or skill level

1273 5. Identify knowledge or skill gaps

1274 Using a specific example, such as implementing multi-factor authentication, the Learning
1275 Program Manager can develop an awareness program for all users in the organization so that
1276 they understand their roles in the program. All users will be expected to adopt multi-factor

authentication on their devices when accessing the organization's systems, and they will be informed of the cybersecurity or privacy benefits and purpose of the methodology. Those with significant cybersecurity and privacy responsibilities will be trained to add this capability to authentication systems and assist personnel at the organization's helpdesk. Senior leadership will participate because they are crucial to ensuring that the goal is well-communicated and supported throughout the organization.

3.1.2.1. Identify Learning Needs

The most important step in initiating a new phase in the CPLP is to establish the learning needs. For example, the organization may be about to introduce new technology, legislation may have been passed that requires personnel to acquire new knowledge or skills, or a new privacy or cybersecurity risk may have emerged that requires the organization to introduce a new learning module. Identifying and prioritizing learning needs will allow the Learning Program Manager to focus their attention on the issues of greatest importance to the organization.

The following techniques can help define the learning needs:

- Identify what knowledge or skills are needed in the organization through a learning needs assessment

- Review existing work or job analysis reports

- Identify any regulatory or other requirements for learning programs

- Review cybersecurity or privacy risks. All organizations face operational risks. While the majority of risk considerations focus on responding to incidents that result in a failure to maintain cybersecurity, it is important to include an effective learning plan as a mitigation factor for risks

- Review lessons learned or after-action reports. After an incident, the Learning Program Manager may be engaged in an effort to educate personnel on corrective best practices. This is an important opportunity to truly learn from mistakes. New material should be developed that not only speaks to the specifics of the incident but may be able to shore up weak areas around it, such as identifying and reporting vulnerabilities

3.1.2.2. Determining the CPLP Audiences

During the analysis phase, the Learning Program Manager will identify and define the audiences to be trained on the identified learning goals. By coordinating with the organization's cybersecurity and privacy learning function, supervisors may be helpful in determining whether personnel need additional training.

Potential audiences for the CPLP include:

- **New employees:** This audience includes contractors, and the focus is usually on the important policies and rules of behavior for the systems that they will access. This training includes what is typically called "new employee orientation" or "on-boarding" and can be joint cybersecurity and privacy training. Some organizations may need to

1314 include a visitor or guest with acceptable use policies if they allow any type of system
1315 access, including wireless network connections.

1316 • **All users:** This is also known as "general workforce training" and includes annual
1317 cybersecurity and privacy training for all organization system users. An analysis of this
1318 audience's training requirements should include a review of the performance of previous
1319 program elements and any new organizational requirements.

1320 • **Privileged users:** These are personnel with additional responsibilities who are trusted to
1321 perform cybersecurity- or privacy-relevant functions that ordinary users are not
1322 authorized to perform. They will require additional training in order to be provided with
1323 privileged access. Some information to consider when identifying privileged users
1324 include:

1325 o Determine whether any new systems have been implemented or are planned, and
1326 identify the rights and privileges associated with privileged account users.

1327 o Review the list of participants with system owners to ensure that the list is
1328 complete and whether new rights and privileges are required.

1329 o Determine whether any of these systems have been moved to the cloud and
1330 require new training.

1331 • **Staff with significant cybersecurity and privacy responsibilities training:** Some
1332 positions with significant responsibilities require highly technical implementation by staff
1333 with significantly specialized responsibilities. This provides additional training that is
1334 designed for a specific job role, task, or responsibility (also known as "role-based"
1335 training). This type of training includes:

1336 o Specialized or customized training on specific products, networks, systems,
1337 applications, or information

1338 o Work role tasks and activities, such as incident response procedures, oversight
1339 responsibilities, or identity management

1340 o Reskilling and upskilling programs

1341 o Learning that helps the employee perform their work tasks

1342 The following are examples of how personnel can be assigned to multiple learning
1343 programs:

1344 o Wilson is currently a system administrator, and as an employee of a federal
1345 agency she attends the annual CPLP training. She is also in the Information
1346 Technology department, so she and her team receive additional training on
1347 cybersecurity and privacy. In her role as a system administrator, she has
1348 significant cybersecurity and privacy responsibilities and is therefore required to
1349 attend additional training.

1350 o Ng is now part of the organization's web publishing team and has access rights to
1351 publish the public-facing webpages of the organization. This carries significant
1352 agency branding and communications responsibilities. Ng must take annual
1353 training and sign an additional Acceptable Use Policy regarding appropriate
1354 publishing activities.

3.1.2.3. Identify the Knowledge and Skills Needed per Participant Type

The primary knowledge and skillset for All Users is the ability to recognize cybersecurity and privacy risks, take appropriate actions to reduce harm to the organization, and report any incidents or events, when appropriate. All Users must be empowered and skilled in adhering to the organization's Rules of Behavior and Acceptable Use Policies, which include guidance on how to use organization-provided devices and access network resources.

Privileged users must possess the knowledge and skills to appropriately use systems that they have been given access to without introducing additional risks or harm to the organization. The training they receive must provide them with the ability to judge risks appropriately.

It is critical to identify the necessary role-based knowledge and skills for those with significant cybersecurity or privacy responsibilities. The NICE Framework can be a useful resource for identifying the knowledge and skills related to specific cybersecurity learning objectives if the learning goal is clear. The NICE Framework includes detailed knowledge and skills statements at a high level related to the work that personnel perform in a variety of cybersecurity work roles. In addition, an organizational job analysis will be useful in determining what the learning objectives are for the program participants. For those with significant privacy responsibilities, the Learning Program Manager should consult with the privacy senior leadership of the organization (i.e., CPO or SAOP) for additional guidance on knowledge and skills required per individual. The Learning Program Manager may also need to consult with managers and subject-matter experts related to the learning goal for additional input on needed knowledge or skills[11].

There are existing models for evaluating the tasks necessary for a particular person's role, such as considering the complexity or difficulty of the task, its importance, and how frequently the task is performed. This is sometimes referred to as the "DIF model" for considering the relative difficulty, importance, and frequency of the task. It can be helpful for identifying the knowledge and skills that the CPLP should focus on when training those with significant cybersecurity or privacy responsibilities.

3.1.2.4. Assess Each Audience's Current Knowledge and Skill Level

After determining the knowledge and skills needed, the next step in the analysis phase is to determine what the audience segment already knows about the topic and skills they possess while keeping the learning goal in mind. The CPLP should focus on providing the learner with the requisite amount of new knowledge and skills while reinforcing existing knowledge and skills.

There are several methods for determining the existing knowledge and skill set:

- Hold guided conversations and interviews with subject-matter experts, managers, system owners, and other organization personnel with relevant mission or business functions.

- Review recent job task analyses.

- Analyze events and related responses that may indicate skill levels.

---

[11] One such resource is the NIST Privacy Workforce Public Working Group which is working to identify and document Tasks, Knowledge, and Skills aligned with the NIST Privacy Framework. https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group

1392   •   Conduct performance-based assessments to evaluate and validate capabilities

1393   These methods can also identify whether new training is needed for a role or roles or whether
1394   existing training needs to be updated or modified.

3.1.2.5.   Identify Knowledge and Skill Gaps

1396   The result of the analysis thus far is a measure of the personnel's existing knowledge and skills
1397   with an overview of each audience segment. The difference between that and the ideal state of
1398   knowledge for the learning goal is referred to as "the learning gap." During the design phase, the
1399   Learning Manager will use information about each learning gap (per learning goal, learning
1400   audience, etc.) to design a program specific enough to address each need.

3.2.   Designing the CPLP

1402   At the beginning of the design phase, consider what knowledge and skills the audience needs to
1403   learn or develop and what gaps the learning material will close. This will drive the creation of the
1404   learning objectives and the process for achieving them. The design process should end with a
1405   systematic blueprint of the approach needed for the CPLP to address the identified knowledge
1406   and skills gaps of the personnel.

3.2.1. The Steps of the Design Phase

1408   The Learning Program Manager begins a formal design phase for the CPLP or a new element in
1409   the ongoing CPLP by creating a Design Document that outlines the requirements. They will then
1410   determine whether they need to build or buy learning materials to satisfy those requirements. The
1411   Learning Program Manager moves into a highly detailed design phase that will lead to the
1412   development of revised or new program assets. The steps in design phase are:

1413   1. Create a Design Document.

1414   2. Conduct an environmental scan of available training, both internal and external.

1415   3. Identify learning objectives.

1416   4. Summarize learning requirements.

3.2.2. Design Document

1418   The Design Document provides a blueprint for the development and implementation of the
1419   learning program elements. The Design Document is usually created by the Learning Program
1420   Manager and reviewed by key stakeholders (when necessary for funding and other approvals)
1421   before moving to the development phase.

1422   Typical elements of a Design Document include:

1423   •   Purpose, goals, and background

1424   •   Intended audience

1425   •   Learning objectives

1426 • Content and environmental scan (e.g., build or buy)

1427 • A course outline, including high-level topics (e.g., number of lessons or modules and
1428   their length)

1429 • An instructional strategy that includes media (e.g., audio, video, demonstrations,
1430   emulations, simulations), activities, and exercises

1431 • Delivery medium (i.e., the learning environment – online, classroom, etc.)

1432 • Types of assessments (e.g., participation, quiz with passing grade, performance-based
1433   skill assessment, etc.)

1434 • Required measurements and metrics

1435 • Signature page to document acceptance from the key stakeholders

1436 Based on its resources, the organization will determine whether it can build, have built, or utilize
1437 existing government or commercial off-the-shelf learning content, which is discussed further in
1438 Section 4.

3.3. Conduct an Environmental Scan of Available Training

1440 The Learning Program Manager will need to determine what training materials have previously
1441 been used in their organization and are still available and appropriate for use. Additionally, there
1442 may be materials and programs available from elsewhere in the organization, agency, or partner
1443 agencies. Federal resources may have materials, presentations, and even speakers available to
1444 satisfy a variety of learning goals. An important result of the environmental scan effort will be
1445 insight into what is currently being done to meet learning requirements in the organization and
1446 the gap in needed program material.

3.3.1. External Sources of CPLP Material

1448 There are a variety of external sources of cybersecurity and privacy learning program material
1449 that can be incorporated into a CPLP. Some possible sources include:

1450 • **Vendors:** If the organization decides to outsource some or all of its CPLP course
1451   development, a number of vendors in the private sector offer "off-the-shelf" courses that
1452   are suitable for particular audiences or that can be developed for specific audiences. Prior
1453   to selecting a particular vendor, agencies should have a thorough understanding of their
1454   CPLP needs and be able to determine whether a prospective vendor's material meets
1455   them. Also, consider who "owns" the material for the purposes of future updates and
1456   adaptations. Be sure to check with the agency contracting officer to ensure that
1457   organizational guidelines are met.

1458 • **Non-profit organizations and grant-based agreements:** Federal organizations may
1459   have agreements with non-profit organizations, grants to universities, or other similar
1460   arrangements for the creation of educational materials on cybersecurity or privacy topics.
1461   Learning Program Managers should be aware of any such opportunities to leverage these
1462   materials.

- **Other organizations:** Organizations can explore the use of CPLP material that has been developed by other organizations and edited to fit their needs rather than developing a completely new course. Care should be taken that the available material is applicable to the intended audience and that the material addresses the learning goals of the organization.

- **Shared events and material:** Several federal agencies offer cybersecurity and privacy learning events that are open to personnel across the government. Learning Program Managers should join federal working groups to remain informed about events, workshops, and conferences intended for professional development.

Sources of timely material may include:

- Email advisories issued by industry-hosted news groups, academic institutions, or the organization's cybersecurity or privacy office

- Cybersecurity or privacy websites

- Themed events, such as Data Privacy Week, Cybersecurity Awareness Month, or Cybersecurity Career Week

- Conferences, seminars, webinars, forums, and courses

3.3.2. Internal Sources of CPLP Material

Within an agency or organization, cybersecurity and privacy Learning Program Managers can build new partnerships or reinforce existing ones with the organization's functional managers who coordinate or conduct their own CPLPs. Functional training developed in-house (e.g., financial applications or personnel management) often lacks adequate discussion of related cybersecurity and privacy issues. Through these cross-departmental partnerships, Learning Program Managers can review existing references to their topic areas in the material and check for completeness and accuracy. The Learning Program Manager can also assist the functional manager by developing a learning module for any material that previously had no cybersecurity or privacy component.

3.4. Identify Learning Objectives: From Analysis to Design

The Learning Program Manager consolidates what they have identified from the review of available materials in order to identify learning objectives for the CPLP. Whether the Learning Program Manager is working on the entire Plan, designing a few new elements, or updating existing elements, this stage can be very useful in ensuring that the effort is closely aligned with identified organizational needs.

3.4.1. Examples of Identifying Learning Objectives

Consider these examples of identified training gaps and their associated learning objectives:

Scenario 1: A recent analysis indicated that on-site, remote, and teleworking employees – including employees with privileged accounts – are using single-factor authentication (i.e., a password). The Chief Information Officer has approved the implementation of a multi-factor

1500 authentication token system starting with privileged accounts in the first quarter and all other
1501 accounts in the second quarter. The CPLP Learning Program Manager has been tasked with
1502 helping employees understand their roles in utilizing this new multi-factor authentication system.

1503 **Analysis Phase: Identify Knowledge and Skill Gaps**

1504 Since this is a new authentication method, both All Users and Privileged Users need
1505 information and training on the new policies, processes, and procedures for accessing the
1506 system. In addition, they need to know why this is important or how it protects the
1507 information and assets on enterprise systems. Privileged Users will also need additional
1508 information focused on the additional privileges they will have once authenticated to the
1509 system.

1510 **Design Phase: Create Learning Objectives Based on Knowledge and Skill Gaps**

1511 Once the knowledge and skill gaps are identified, the next step is to establish the learning
1512 goals and objectives for the program. In this example, the goals and objectives for the
1513 learning program involve enabling employees to:

1514 • Understand the vulnerabilities associated with using single-factor authentication
1515 (e.g., user ID and password)

1516 • Understand why the organization is using a multi-factor authentication token
1517 method

1518 • Identify their role in using multi-factor authentication

1519 • Install the authentication application and verify that the token is received

1520 • Utilize the token 100 % of the time for authentication to the system

1521 **Scenario 2:** A recent external audit of the organization's system privacy policies and practices
1522 highlighted several concerns. The top issues were that (1) the public privacy notice indicated that
1523 PII was only being shared with certain entities, when in fact it was being shared with other
1524 entities as well; (2) Information System Privacy Officers and Managers (ISPO/ISPMs) had too
1525 many systems to oversee, monthly data processing reports were not reviewed in a timely manner,
1526 and management was not receiving reports of critical problematic data actions; and (3) the
1527 financial office employees were not adequately protecting the privacy of employee bank
1528 information when processing the employees' travel costs.

1529 **Analysis Phase: Identify Knowledge and Skill Gaps**

1530 During the analysis phase, the CP Learning Manager determined the following:

1531 • Systems owners of systems processing PII are designated as employees with
1532 significant privacy responsibilities and participate in an annual three-hour
1533 customized seminar that includes new policies, privacy risk briefings, and
1534 network opportunities. During the next version of the existing training, additional
1535 content on verifying how PII is being process comports with the public privacy
1536 notice will be added.

1537 • While the ability to review monthly data processing reports may be a resource
1538 issue, no training gap is determined at this time. Further analysis would be needed
1539 to determine whether ISPO/ISPMs were able to identify critical problematic data

1578 • Program elements should meet accessibility standards.

1579 • Require the ability to update and maintain content to stay current.

1580 • Ensure that the material works for different audience types and sizes.

1581 • Recognize and support the diversity of the workforce.

1582 • Provide an overview of what class participants can expect to learn after progressing
1583 through the learning materials.

1584 • Establish learning objectives in accordance with the organizational mission.

1585 • Dedicate a separate section to each learning objective and create individual lessons for
1586 each of the learning objectives.

1587 • Integrate visual elements, such as graphics, videos, tables, and other visual tools to
1588 reinforce important concepts.

1589 • Use interactions to engage the audience and promote their ability to transfer content from
1590 the training environment to the workplace.

1591 • Enable managers and supervisors to check progress, run reports, and access the LMS.

1592 • Support required reporting needs for the executive leadership.

1593 • Ensure that the IT and help desk staff receiving training to support the CPLP.

1594 • If using outsourced courses, ensure that vendors are supported and can update the
1595 reporting and LMS platforms.

1596

1597

4. Development and Implementation of the CPLP

Once the CPLP requirements have been established and documented in the design phase, the Learning Program Managers can proceed to develop the Program. This phase is where each audience's requirements are evaluated, budgeted, and provided for separately. Typically, the requirement to develop an All User CPLP will be well-understood and may already exist. Determine whether that is true, whether the program requires significant investment to be updated, and whether the talent and expertise are available to support the needed work.

The development process will involve various personnel, including:

- **Management:** All levels of management will be responsible for their staff learning needs, the prioritization of training resources, the identification of training gaps, and evaluation of the training's effectiveness.

- **Cybersecurity and privacy specialists and subject-matter experts:** Specialists and subject-matter experts help determine the task, knowledge, and skill requirements of the roles or job functions, identify training gaps and needs within the organization, and guide the development and review of learning materials.

- **Training professionals:** Training professionals acquire, customize, develop, present, and evaluate the training content and training programs. Whether the training team and cybersecurity and privacy teams are in the same department or not, the groups will work closely together, along with other subject-matter experts to ensure the relevance and accuracy of the material and programs.

- **Acquisitions and budget:** These departments will be engaged when circumstances and needs require the development or acquisition of externally sourced services or content.

Once the baseline requirements of the program have been solidified, a feedback strategy can be designed and implemented to ensure that materials continue to support the CPLP strategy and address identified training needs.

4.1. Developing CPLP Material

After the Learning Program Manager has completed their analysis and design reviews, they will have a comprehensive set of Design Documents to guide the development of new materials. These documents are useful when allocating budgets and personnel for the creation of new materials or program elements. However, additional information will be needed to guide the content creators in their work.

4.1.1. Create a Requirements Document for Sourcing New Material

If the Learning Program Manager determines that it is necessary to create or source new CPLP content, curricula, or other program elements, they will need to create a Requirements Document. The Requirements Document incorporates the information from the Design Document as well as any additional and necessary information to provide to the training and curricula developers, editors, and designers, whether they are in-house or vendors. The Requirements Document will also be useful for the organization's acquisition and budget functions.

1637 The Requirements Document provides detailed and specific criteria related to the content needed
1638 to meet the learning objectives. Typical prompts or questions to review when creating the
1639 Requirements Document include:

1640 • What specific cybersecurity or privacy risks does the organization seek to address or
1641 reduce?

1642 • What knowledge or skills should the learner acquire or improve as a result of the CPLP
1643 element?

1644 • What behaviors need to be addressed or reinforced?

1645 • Does the material contribute to a positive cybersecurity and privacy culture that
1646 reinforces the role of all users in reducing organizational risk?

1647 • Will the material engage personnel?

1648 • What are the budget requirements and timing?

1649 • Who in the organization will be included in reviews of content development and
1650 approvals?

1651 • What sort of user testing will be conducted to ensure content is appropriate for the
1652 Learning Program participant; meets their needs and is appropriate to their skill level.

1653 ### 4.1.2. Developing the All User Learning Program

1654 The All User Learning Program elements, as described in Section 2.5.1, are delivered throughout
1655 the year. However, there may be necessary updates to and iterations of the content based on
1656 events and organizational requirements. Ensure that the budget is allocated to update the content
1657 or amend the materials with other delivery methods (e.g., to video training) if making actual
1658 content changes would be cost prohibitive.

1659 The challenge of developing a dynamic and effective All User Learning Program – and
1660 particularly, the cybersecurity and privacy presentation – is that the audience is aware of the
1661 compulsory nature of the program so the materials and presenters must be engaging and hold
1662 their attention. There is much at stake given the ever-changing nature of cybersecurity and
1663 privacy risks to the organization, especially when learners arrive with an expectation that they
1664 only need to do the bare minimum to fulfill their training requirement. However, there will
1665 almost always be new and crucial content for them to understand and master in order minimize
1666 the organization's risk.

1667 Consider how key messages will be reinforced throughout the All User Learning Program.
1668 Whether it is part of an annual event or shared on awareness materials, repeated messages
1669 become retained messages. Use the awareness program materials to keep the All User Learning
1670 Program topical without becoming repetitive or intrusive. This is a tricky balance to achieve and
1671 requires a variety of delivery formats and messages. Consider varying the awareness program
1672 techniques, such as sending out cybersecurity or privacy topic emails on a monthly basis, adding
1673 a campaign message to everyone's official organization signature block for Cybersecurity
1674 Awareness Month in October, or Data Privacy Week in January, or place posters in the agency's
1675 lunchroom all year round.

1676 There are many techniques for disseminating cybersecurity and privacy awareness messages
1677 throughout an organization. Choosing those techniques depends on available resources and the
1678 complexity of the messages. Some techniques that are appropriate for a single message include
1679 posters, screensavers, warning banners, organization-wide emails, brown bag seminars, and
1680 awards programs. Techniques that can more easily include several messages or themes include
1681 "do and don't" lists, email newsletters, web-based sessions, teleconferencing sessions, in-person
1682 instructor-led sessions, and email signature messaging. Examples of awareness material can be
1683 viewed on the Federal Information Security Educators (FISSEA) website[12] under Contests for
1684 Awareness and Training.

1685 Additional considerations when developing the All User Learning Program:

1686 • What does the organization want all personnel to be aware of regarding cybersecurity and
1687 privacy? Starting points may include a review of the latest top risks to the organization,
1688 as reported by the information security or privacy office; common risks reported by
1689 cybersecurity and privacy organizations; and new mission goals with cybersecurity or
1690 privacy implications. Evaluating organizational policies, program reviews, internal
1691 audits, internal controls program reviews, self-assessments, and spot-checks can also help
1692 Learning Program Managers identify additional topics to address.

1693 • Were constraints found in the Analysis? For example, does the organization have
1694 particular issues with delivering a Learning Program to personnel? Will personnel be able
1695 to access or attend training by a particular required date to achieve completion? Are some
1696 personnel working remotely, traveling, located overseas, or require reasonable
1697 accommodations? Consider what additional steps will be needed to ensure that all
1698 personnel can participate in the All User Learning Program and fulfill their Learning
1699 Program obligations.

4.1.3. Developing a Privileged Users Learning Program

1700

1701 The steps for this phase are similar to developing the All Users Learning Program. Create a
1702 Requirements Document that aligns learning goals for this audience with available funding as
1703 well as organizational requirements.

1704 Additional considerations for Developing the Privileged User Learning Program:

1705 • What do we want privileged users to be aware of regarding cybersecurity and privacy?

1706 • What procedures do personnel need to follow to adequately protect their privileged
1707 accounts?

1708 Some starting points include understanding the rights and privileges allotted to this group,
1709 reviewing the risks related to privileged accounts or the systems or applications associated with
1710 privileged access, reviewing these issues with the CIO or CISO's office, and aligning learning
1711 goals for these risks to the available budget for impacted personnel and departments. Evaluating
1712 organizational policies, program reviews, internal audits, internal controls program reviews, self-
1713 assessments, and spot-checks can also help Learning Program Managers identify additional
1714 topics to address.

---

[12] https://www.nist.gov/itl/applied-cybersecurity/fissea

4.1.4. Developing a Learning Program for Those With Significant Cybersecurity and Privacy Responsibilities

The more customized and individualized nature of ongoing skills development and training for personnel with significant cybersecurity and privacy responsibilities will require a more detailed and nuanced Learning Program approach. For example, it may require multiple Requirements Documents for developing new Learning Program elements and identifying training that will satisfy learning objectives. The Learning Program Manager will partner and coordinate these efforts with the organization's human capital office, Chief Learning Officer, training and curriculum developers, and the individual managers and supervisors for the personnel in this group.

Various methods for developing or identifying role-based training for these users are available to the Learning Program Manager. They should ensure that the complexity of the training is commensurate with the role and needs of the people who will undergo the learning effort. Cybersecurity and privacy role-based training material can be developed at a beginning level for a person who is just learning a discipline. Material can be developed at an intermediate level for someone who has more experience and, therefore, more responsibility in their workplace. Advanced material can be developed for agency subject-matter experts whose jobs incorporate the highest level of trust and an accompanying high level of cybersecurity or privacy responsibilities.

4.1.5 Conducting User Testing on new CPLP Elements

Include a user testing phase for all new CPLP elements prior to implementation. Content should be assessed for each learning program participant group to ensure it meets their needs and is appropriate to their skill level. Additional user testing might include evaluating the intended element's delivery method, the appropriateness of the language, the value to the learner, overall acceptance of the new element. Feedback from user testing should be iterative and incorporated at every step of the design effort, not just in the form of evaluations after implementation.

4.2. Implementing New CPLP Elements

Implementation refers to the actual distribution and delivery of the CPLP material. This phase focuses on the connection between the learner and the content. Once the plan for implementing the CPLP has been communicated to and accepted by management (see Section 2.11), the implementation phase can begin. Use a life cycle process when implementing the program to avoid a "one and done" scenario and periodically review the program for updates and corrections.

4.2.1. Steps for Implementing a new CPLP Element

The Learning Program Manager should implement a new Learning Program or a single element with the same repeatable steps. It is of the utmost importance that all of those involved in the implementation phase be included in a well-designed communications effort. This ensures that personnel and their managers or supervisors are well-informed about any upcoming CPLP opportunities that are relevant to their required learning plan. The implementation phase is also

1754 the time to confirm that the required reporting and metrics can be satisfied in later program
1755 phases. Steps to consider before initiating the implementation phase include:

1756   1. Communicate the CPLP implementation

1757   2. Plan to measure success by establishing measurement, metric, and reporting requirements

1758   3. Build a CPLP schedule

1759   4. Plan to evaluate program success by reviewing post-implementation
1760   feedback, measurements, and metrics

4.3. Communicating the CPLP Implementation

1762 Communication is a large part of developing an organization's shared culture of supporting the
1763 Learning Program efforts. The Learning Program Manager should develop a Communications
1764 Plan for each phase of the program element implementation and include the organization's
1765 communication team. The Learning Program Manager should determine the appropriate timing
1766 to inform managers, supervisors, and possibly the personnel involved about upcoming and
1767 required Learning Program elements, as well as the frequency with which to send out reminders
1768 and other forms of communication that encourage cooperation from the organization.
1769 Communication is a large part of developing an organization's shared culture of supporting the
1770 Learning Program efforts.

1771 Each individual CPLP element (e.g., presentation, course, or tabletop exercise) requires a
1772 separate and more detailed form of communication to inform the learners and their managers of
1773 the following:

1774   • Purpose of the training or learning activity

1775   • Participating employee groups (if not all users)

1776   • Consequences of not completing the training (by deadline or at all)

1777   • Course title

1778   • Delivery method (e.g., in person, virtual delivery, self-directed online learning, etc.)

1779   • Required or recommended accommodations

1780   • Tracking method (and completion tracking)

1781   • Availability date

1782   • Due date

1783   • Verification of users with significant cybersecurity responsibilities

1784   • How to request accommodations

1785 The Communications Plan should include a clear explanation of why the training is being
1786 mandated or encouraged. Applicable federal legislation, regulations, and internal (agency or
1787 organizational) policies should be referenced.

1788 Each category of user must be specified for the training assigned. For example, if the
1789 organization's policy states that all IT users must complete a particular training to gain or

1790 maintain access to IT systems, the communications plan must include this notice. For those with
1791 significant cybersecurity or privacy responsibilities, identify which training is assigned to a
1792 specific work role, individual, or department.

1793 Employees must know the consequences of failing to complete the learning activity according to
1794 the organization's policy. This should be explained in the Learning Program Communications
1795 Plan and noted in the course description in the Learning Plan within the Learning Management
1796 System.

1797 Other considerations for CPLP communications include:

1798 • Course titles and numbers should be unique, differentiated, and include information on
1799   the access method (e.g., online or in-person), availability, course dates, and deadlines.

1800 • All learners, their managers or supervisors, and human capital departments should be
1801   made aware of any required training and associated due dates. Communication should
1802   include reminder messages, references and links to the organization's official policy
1803   statements for employee information systems, and the consequences for failing to
1804   complete the learning activity.

1805 ## 4.4.   Establishing Reporting and Metrics Requirements for CPLP Elements

1806 The Learning Program Manager should strive to ensure that the implementation of all new CPLP
1807 elements (e.g., courses, training, posters, practical exercises, etc.) will allow for performance
1808 metrics and measurements to be established and collected. Establish these requirements during
1809 the developmental phases of both the overall program and each component for which measures
1810 are expected to meet regulatory and annual reporting requirements and to continually assess and
1811 improve the performance of the program. As previously mentioned in Section 3.2.2, these must
1812 be included in the Design Plan requirements that go to curriculum and content developers.

1813 In addition to any applicable measures that support the program, as described in Section 2.4, the
1814 Learning Program Manager should utilize element level measures, such as the target percentage
1815 of the applicable audience who receives the training or awareness material and feedback from the
1816 audience on effectiveness of the material.

1817 Some considerations for reporting:

1818 • Learning Management System (LMS) integration: Training is usually tracked and
1819   recorded using the LMS. Will the course or training element include quizzes with scores
1820   or other metrics and measurements?

1821 • Non-LMS integrated elements: Consider how the participation and performance of each
1822   learner will be tracked and recorded if the training is face-to-face, virtual, or hybrid. Will
1823   manual or paper tracking be required?

1824 ## 4.5.   Building a CPLP Schedule

1825 Establish a primary calendar for CPLP activities. The process may be automated using an LMS.
1826 Enable organization-wide access so that personnel can find elements applicable to each audience
1827 segment (e.g., by date, learning objective, etc.). It is a good idea to align this calendar with the

1828   Communications Plan to be able to send out reminder communications and ensure that
1829   instructors and materials are identified and allocated well in advance.

1830   **4.6.   Determining Post-Implementation Activities**

1831   Once any CPLP element has been delivered or implemented, the post-implementation activities
1832   that fuel assessment and improvements should be managed. These will include:

1833   • Sending post-training feedback surveys

1834   • Conducting instructor feedback surveys

1835   • Determining attendance and completion rates

1836   • Other mandated or organizational reporting

1837   • Budget reconciliation (i.e., did the CPLP element implementation meet budget
1838   requirements or go over or under?)

1839   For some awareness elements, measuring audience engagement is less straightforward,
1840   especially for passive items like posters or email signatures. Nevertheless, it is possible to
1841   measure impact. One method could include surveying a sample of users to discuss their
1842   familiarity with the messaging or whether they have practiced any of the tips.

1843

1844

1845 **5.   Assessment and Improvement of the CPLP**

1846 An effective CPLP meets the needs of the learners and the organization by measuring and
1847 evaluating the performance of the Program on a continual basis. This requires up-to-date
1848 knowledge, awareness, and understanding of the legal and regulatory compliance requirements
1849 for the organization and the cybersecurity and privacy risks that may impact the organization.
1850 The Learning Program Manager works with organizational leaders, training staff, and learners to
1851 share performance reporting and decision-making throughout all phases of the CPLP. Both the
1852 analysis of organizational risks (e.g., employee responses to practical exercises) and review of
1853 the efficacy of material (e.g., learner feedback responses to courses) are important in the
1854 continual improvement of a CPLP in an evolving threat landscape.

1855 **5.1.   Steps for Assessing and Improving the CPLP**

1856 The process for assessing and improving the CPLP may vary by organization and available
1857 resources. Consider the following steps before evaluating the CPLP's performance, whether for
1858 the entire CPLP, per audience segment, or for a single CPLP element, such as a new training
1859 course:

1860   1. Create a CPLP Assessment Report

1861   2. Agree on the changes needed to the CPLP

1862   3. Evaluate budget requirements for program improvement

1863   4. Review and update the strategic plan

1864   5. Implement changes into the next revisions of the program elements and schedule

1865 **5.2.   Create a CPLP Assessment Report**

1866 At the end of a campaign, each quarter, or annually, the Learning Program Manager should
1867 create a summary document that is suitable for review with senior leadership. This report will
1868 provide an analysis of attendance, feedback, measurements, and other metrics and help to
1869 identify action items, areas of improvement, and next steps. It should be tailored for the senior
1870 leadership reader, using language and framing that is appropriate. Avoid using technical jargon
1871 without explanation.

1872 Key elements of an Assessment Report include:

1873   • Measurements and metrics

1874   • Compliance information

1875   • Evaluating CPLP effectiveness

1876   • CPLP improvement efforts

1877 The Learning Program Manager will have established their Program Metrics Plan during the
1878 planning stage (see Section 2.4) and should strive to include a number of different quantitative
1879 and qualitative tools. Metrics are an important and effective tool for determining an
1880 organization's cybersecurity and privacy learning needs. Metrics monitor the accomplishment of
1881 the program goals and objectives by quantifying the level of implementation, effectiveness, and

1882   efficiency of the program while identifying possible improvements. Include results from both
1883   quantitative and qualitative measurement instruments.

5.2.1. Compliance Reporting

1885   One element of the report is to indicate whether the CPLP has met the regulatory compliance
1886   requirements for the organization. The Learning Program Manager should be aware of all
1887   regulations that require reports to be created for their organization. As a subject-matter expert on
1888   the topic of providing training programs for the agency or organization's employees, the
1889   Learning Program Manager should typically engage in self-development processes that maintain
1890   an awareness of these needs. In some organizations, this may all be handled by a single
1891   individual or group that is assigned to manage legal and regulatory compliance. For those
1892   organizations where the duties are separated, it is critical to maintain collaborative
1893   communication to ensure that the program meets compliance.

1894   A fully developed and integrated CPLP may become a useful tool for supporting enterprise risk
1895   management, although many are initially developed to address compliance requirements in laws,
1896   regulations, policies, or standards. Meeting these compliance measures is often the primary focus
1897   of higher level leadership, but should be only the starting point for a robust CPLP program.
1898   Examples of common quantifiable metrics to demonstrate CPLP compliance include training a
1899   certain percentage of the workforce and the results of practical exercises. Organizations should
1900   determine which compliance measures they must achieve and consider those inputs when
1901   developing the CPLP.

1902   Learning Program Managers should work with policy owners to ensure that the results of the
1903   learning efforts satisfy compliance requirements. The CPLP needs to build in methods that allow
1904   for this type of reporting. That conversation could include questions such as:

1905   • Which personnel received (or participated in) the learning element?

1906   • How well does the participation level match the goal of user coverage?

1907   • How far should the CPLP go in pursuit of expected coverage?

1908   • Have individuals in compliance-identified roles met their learning requirements?

5.3. Evaluating CPLP Effectiveness

1910   Because the focus of this program is on learning and mastering content, it is important to analyze
1911   issues that are typically assigned to the learning and educational branch of the organization. The
1912   cybersecurity and privacy Learning Program Manager needs to be involved in the creation of
1913   course material to ensure that it is accurate, relevant, and timely. This requires analyzing the
1914   accuracy, quality, and appropriateness of delivery of the material in the context of the desired
1915   outcomes. The Learning Program Manager should expect to take an active role in course
1916   development and to follow up after teaching to determine whether the material was delivered as
1917   intended.

1918   Another primary goal of a CPLP is to empower users to demonstrate better decision-making
1919   behaviors. While these types of behavioral improvements tend to be more difficult to measure,

1920 working with functional managers and other staff may help in the development of measurable
1921 objectives to assess behavioral changes.

5.3.1. Instructor Evaluation

1922

1923 Each CPLP will determine whether they can support a dedicated in-house team of instructors.
1924 Others may need to use contractors to implement courses and training. In some organizations, the
1925 cybersecurity Learning Program Manager is also the privacy Learning Program Manager and
1926 lead instructor for all of the above. Regardless of the size of the organization, it is important to
1927 consider the required skills of the instructor. Learning Program Managers should work with
1928 leadership to find the right instructors for their personnel and their CPLP's learning objectives. It
1929 is also important to monitor the performance of instructors via observation and other forms of
1930 feedback.

1931 Instructors can also give feedback on the learning material. Learning Program Managers should
1932 work with the instructors to review the material for effectiveness. Instructors frequently provide
1933 feedback on:

1934 - Perceived accuracy

1935 - Ease of instruction and ease of learner understanding

1936 - Adequacy of materials to support content

1937 - Relevance and timeliness of materials

5.3.2. Learner Performance and Feedback

1938

1939 An effective CPLP will include evaluations of learner performance and ask personnel for
1940 feedback.

1941 There are many techniques for addressing how well the learner has absorbed the content and will
1942 be able to apply it. The most common technique for measuring learner performance is the use of
1943 in-course or post-course evaluations. Questions or assessments should be developed at a level
1944 commensurate with both the complexity of the material and the level of understanding expected
1945 of the learner. Note: these evaluations won't show whether there was long-term learning or
1946 application of that learning. Refer back to other ways of measuring employee behaviors as a
1947 long-term way to measure learner performance. Additionally, these measures should be
1948 aggregated across the workforce or a group, not necessarily attributed to a unique learner.

1949 As needed, the Learning Program Manager should work with other functional managers to
1950 identify weaknesses in the knowledge and skills of personnel, whether individually or by role, to
1951 determine where results do not match the goals and learning objectives for each training element.

1952 Helping personnel to provide CPLP feedback is recommended for encouraging a sense of shared
1953 responsibility in the cybersecurity and privacy culture of the organization. Learning Program
1954 Managers should consider how they can provide easy feedback mechanisms throughout their
1955 program.

5.3.3. Review of the CPLP Assessment Report With Senior Leadership

As a final step, the Learning Program Manager will meet with the Senior Leadership Committee to review the performance of the program, address new organizational risks or concerns to include in the training program content, and identify any areas for significant improvement. This phase helps to ensure that the cyclical approach depicted in **Fig. 1** is an ongoing and continual effort.

5.4. Continuous Monitoring and Improvement

NIST SP 800-53, section 1.3, includes the organizational responsibility of "[c]ontinuous monitoring of information systems and organizations to determine the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of security and privacy organization-wide." In this context, the continuous monitoring and improvement refers to the iterative nature of reviewing, updating, and maintaining the program in alignment with requirements and best practices. Based on the CPLP Assessment Report and any new requirements (e.g., legislative, organizational, system changes, risk-related, etc.), the Learning Program Manager will be able to identify opportunities for improvement. As part of the iterative nature of a CPLP, the assessment and continual improvement process can happen during any phase of the CPLP. Continual improvement is simply the concept of periodically revisiting each step of planning, design, development, and implementation to ensure that the CPLP meets the identified goals and requirements in the strategic plan. The continual improvement process does not imply inherent shortfalls in the program. Rather, it acknowledges the constantly shifting needs of an organization to manage resources and risks.

Ultimately, the goal of the CPLP is to enable the organization to withstand cybersecurity and privacy-related risks to information and assets. The personnel of the organization are a crucial part of creating the positive cultural norms that will both support the aims of the CPLP and contribute to greater success in changing behaviors. Avoid efforts to penalize those who do not adapt to the culture as well as others. Rather, shine a light on teams and departments that improve performance or establish best practices. Find ways to celebrate personnel who are building the organization's CPLP culture, and share information about the CPLP's performance when appropriate. If feedback indicates that a change is required to the training because something is not working, ensure that the program is nimble enough for that adjustment to be implemented. Do not wait for the end of the year or another arbitrary time period.

The goals of continual improvement do not need to be built on the ashes of past failures but should be seen as an opportunity to grow and strengthen a critical program. A positive cybersecurity and privacy culture celebrates successes while acknowledging the ever-present risks to the organization.

1993 **References**

1994 [1] Office of Management and Budget (OMB) Circular A-130 (2016), *Managing Information*
1995 *as a Strategic Resource.* Available at
1996 https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a1
1997 30revised.pdf
1998 [2] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,
1999 Public Law 116-283. Available at https://www.congress.gov/116/plaws/publ283/PLAW-
2000 116publ283.pdf
2001 [3] Petersen R, Santos D, Wetzel K, Smith M, Witte G (2020), Workforce Framework for
2002 Cybersecurity (NICE Framework). (National Institute of Standards and Technology,
2003 Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1.
2004 https://doi.org/10.6028/NIST.SP.800-181r1
2005 [4] Grance, T, Nolan T, Burke K, Dudley R, White G, Good T (2006), Guide to Test, Training,
2006 and Exercise Programs for IT Plans and Capabilities, 1.0 (National Institute of Standards
2007 and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. Available at
2008 https://doi.org/10.6028/NIST.SP.800-84
2009 [5] National Institute of Standards and Technology (2018) Framework for Improving Critical
2010 Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology,
2011 Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.6
2012 [6] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool
2013 for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National
2014 Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White
2015 Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10
2016 [7] deZafra DE, Pitcher SI, Tressler JD, Ippolito JB (1998) Information Technology Security
2017 Training Requirements: a Role- and Performance-Based Model. (National Institute of
2018 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-16.
2019 https://doi.org/10.6028/NIST.SP.800-16
2020 [8] Joint Task Force (2018) Risk Management Framework for Information Systems and
2021 Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute
2022 of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37,
2023 Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2
2024 [9] Joint Task Force (2020) Security and Privacy Controls for Information Systems and
2025 Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
2026 Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020.
2027 https://doi.org/10.6028/NIST.SP.800-53r5
2028 [10] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073.
2029 Available at https://www.govinfo.gov/app/details/PLAW-113publ283
2030 [11] Haney J, Jacobs J, Furman S, Barrientos F (2022) Approaches and Challenges of Federal
2031 Cybersecurity Awareness Programs. (National Institute of Standards and Technology,
2032 Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8420A.
2033 https://doi.org/10.6028/NIST.IR.8420A
2034 [12] Haney J, Jacobs J, Furman S, Barrientos F (2022) The Federal Cybersecurity Awareness
2035 Workforce Professional Background Knowledge, Skills, and Development Activities.
2036 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report
2037 (IR) NIST Interagency or Internal Report 8420B. Available at
2038 https://doi.org/10.6028/NIST.IR.8420B

2039   [13] FY2021 Inspector General Federal Information Security Modernization Act of 2014
2040   (FISMA) Reporting Metrics v1.1 (2021). Available at
2041   https://www.cisa.gov/sites/default/files/publications/FY%202021%20IG%20FISMA%20Me
2042   trics%20Final%20v1.1%202020-05-12.pdf
2043   [14] NIST Glossary https://csrc.nist.gov/glossary
2044   [15] Information Technology Reform Act of 1996, 40 USC 11101; Sec. 5002: Definitions.
2045   Available at https://www.govinfo.gov/content/pkg/USCODE-2021-title40/pdf/USCODE-
2046   2021-title40-subtitleIII-chap111-sec11101.pdf

2047 **Appendix A. Examples of Cybersecurity and Privacy Learning Program Maturity Levels**

2048 The following example is adapted from the FY21 Inspector General FISMA Metrics for Security Training [12] and provides one
2049 method for assessing the maturity of a Learning Program. Similar to other business or quality maturity models, this example can help
2050 measure progress and set strategic goals for optimizing the Learning Program. A fully "mature" program is an integrated operational
2051 element of the system and processes and is continually monitored and improved.

Question	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
The extent to which the roles and responsibilities of the Learning Program have been defined, communicated, implemented, and appropriately resourced	Roles and responsibilities have not been defined, communicated, or implemented across the organization nor appropriately resourced.	Roles and responsibilities have been defined, communicated, and implemented across the organization, and resource requirements have been established.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources are allocated in a risk-based manner for stakeholders to consistently implement, and stakeholders are held accountable for carrying out their roles and responsibilities effectively.	
The extent to which the organization utilizes an assessment of the skills, knowledge, and abilities of its workforce to provide tailored and specialized learning content	The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	The organization has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its learning needs. It periodically updates its assessment to account for a changing risk environment.	The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its learning content; and identified its skill gaps. It periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's learning strategy and plans.	The organization has addressed its identified knowledge, skill, and ability gaps through training or talent acquisition.	The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.
The extent to which the organization utilizes a learning strategy and plan that leverage skills assessment and are	The organization has not defined its security learning strategy or plan for developing, implementing, and	The organization has defined its learning strategy and plan for developing, implementing, and	The organization has consistently implemented its organization-wide	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its	The organization's Learning Program activities are integrated across other security-related domains. For

Question	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
adapted to the organization's mission and risk environment.	maintaining a Learning Program that is tailored to its mission and risk environment.	maintaining a Learning Program that is tailored to its mission and risk environment.	learning strategy and plan.	learning strategies and plans. The organization ensures that data-supporting metrics are obtained accurately, consistently, and in a reproducible format.	instance, common risks, control weaknesses, and other outputs of the agency's risk management and continual monitoring activities inform any updates that need to be made to the Learning Program.
The extent to which the organization ensures that the Learning Program is provided to all personnel and is tailored based on its mission, risk environment, and types of information systems	The organization has not defined its learning policies, procedures, or related material based on its mission, risk environment, or the types of information systems that its users have access to.

The organization has not defined its processes for ensuring that all personnel are provided with training upon initial access to the system and periodically thereafter.

The organization has not defined its processes for evaluating or obtaining feedback on its Learning Program to make continual improvements. | The organization has defined and tailored its learning policies, procedures, related material, and delivery methods based on identified requirements and the types of information systems that its users have access to.

The organization has defined its processes for ensuring that all personnel, including contractors, are provided with training upon initial access to the system and periodically thereafter.

The organization has defined its processes for evaluating and obtaining feedback on its Learning Program and uses that | The organization ensures that its learning policies and procedures are consistently implemented.

The organization ensures that all appropriate users complete the organization's training upon initial access to the system and periodically thereafter and maintains completion records.

The organization obtains feedback on its Learning Program and uses that information to make improvements. | The organization measures the effectiveness of its Learning Program by, for example, conducting practical exercises and following up with additional awareness, training, or disciplinary action, as appropriate.

The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its learning policies, procedures, and practices.

The organization ensures that data-supporting metrics are obtained accurately, consistently, and in a reproducible format. | The organization has institutionalized a process of continual improvement that incorporates advanced learning practices and technologies.

On a near real-time basis, the organization actively adapts its learning policies, procedures, and processes to a changing cybersecurity and privacy landscape and provides learning content, as appropriate, on evolving and sophisticated threats and problematic data actions. |

Question	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
		information to make continual improvements.			
The extent to which the organization ensures that specialized learning is provided to individuals with significant security or privacy responsibilities	The organization has not defined its security or privacy learning policies, procedures, or related materials based on its mission, risk environment, or the types of roles with significant security or privacy responsibilities. The organization has not defined its processes for ensuring that personnel with significant security or privacy roles and responsibilities are provided with specialized learning content and does not offer additional learning opportunities.	The organization has defined its security and privacy learning policies, procedures, and related material based on its requirements, mission, risk environment, and the types of roles with significant security and privacy responsibilities. The organization has defined its processes for ensuring that personnel with assigned security and privacy roles and responsibilities are provided with specialized security learning material and periodically given additional learning opportunities.	The organization ensures that its security and privacy learning policies and procedures are consistently implemented. The organization ensures that individuals with significant security and privacy responsibilities complete the organization's defined specialized learning and are provided with periodic enhancements or additional relevant learning opportunities. The organization maintains completion records for specialized learning taken by individuals with significant security and privacy responsibilities. The organization obtains feedback on its security and privacy Learning Program and uses that information to make improvements.	The organization ensures that its security and privacy learning policies and procedures are consistently implemented. The organization ensures that individuals with significant security and privacy responsibilities complete the organization's specialized security and privacy learning and provides periodic enhancements and additional relevant learning opportunities. The organization maintains completion records for specialized learning taken by individuals with significant security and privacy responsibilities. The organization obtains feedback on its security and privacy Learning Program and uses that information to make improvements.	The organization has institutionalized a process of continual improvement that incorporates advanced security and privacy learning practices and technologies. On a near real-time basis, the organization actively adapts its security and privacy learning policies, procedures, and processes to a changing cybersecurity and privacy landscape and provides learning material, as appropriate, on evolving and sophisticated threats and problematic data actions.

2052

Appendix B. Glossary

Other terms not defined herein may be found in the NIST Glossary [13].

awareness
The ability of the user to recognize and avoid behaviors that could compromise cybersecurity and to act wisely and cautiously to increase cybersecurity.

awareness content
Content that is designed and implemented to help employees realize how their actions may impact or influence vulnerabilities and threats. Organizations provide various types of awareness material (e.g., posters, newsletters, websites) so that employees can realize their roles in protecting cyber assets.

awareness training
The foundational cybersecurity or privacy training program for all personnel. It is designed to help users understand the role that they play in protecting information, cybersecurity, and privacy-related assets. It often consists of instructor-led, online courses, exercises, or other methods that inform users of the acceptable use of and risk to the organization's systems.

> *Note:* This is referred to as "literacy" training in the NIST SP 800-53 Awareness and Training (AT) control family [8].

> Also see: *training*.

certification
A designation earned to ensure qualifications to perform a job or task. Often issued by a professional organization, industry vendor, or employer to signify an achievement following a course of study.

Chief Data Officer
A senior executive responsible for the utilization and governance of data across the agency or organization.

Chief Financial Officer
A senior member responsible for managing the financial actions of an agency or organization.

Chief Learning Officer
A senior-level executive who oversees all learning and employee development programs within an agency or organization.

Chief Privacy Officer
The senior official who is designated by the head of each agency and has agency-wide responsibilities for privacy, including the implementation of privacy protections; compliance with federal laws, regulations, and policies related to privacy; the management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

competency
An individual's ability to complete a task or tasks within the context of a work role.

> From OPM: A *competency* is a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully. Competencies specify the "how" of performing job tasks, or what the person needs to do the job successfully.

> Additional information is available at https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/.

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

cyber range

This technique provides a safe environment (sandbox) to deliver hands-on realistic training, scenarios, challenges, and exercises in an easy-to-access web-based environment.

cybersecurity

The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

Data privacy

a condition that safeguards human autonomy and dignity through various means including confidentiality, predictability, manageability, and disassociability.

Data Management Officer

Responsible for overviewing and carrying out the data management tasks of research projects. Main duties and responsibilities include data collection, or the formulation, implementation, and enforcement of proper data collection policies and procedures. Trains reporting agencies on data collection tools and equipment.

disassociability

Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

gap analysis

The process of comparing current Learning Program or activity performance with the desired, expected performance.

information technology

(A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use— (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract. [14]

integrity

Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.

learning objectives

Identifies the outcomes that the learning program sub-component or module should strive to meet for each of the participants and their associated roles. which helps to build an understanding of risks and explain everyone's role in reducing, managing, and mitigating risks.

Learning Program

Consists of numerous elements led by the Learning Program Manager(s), who develop a Strategic Plan to deliver a right-sized program to reduce organizational cybersecurity and privacy risks via workforce education and training. The Learning Program operates throughout the year and incorporates plans for ongoing improvements that are based on rigorous assessments and metrics that support compliance and other mandated reporting. A supportive objective is to develop a positive cybersecurity and privacy culture and not to blame or shame the workforce for lapses or errors.

Learning Program Management

The people and processes that support the cybersecurity and privacy Learning Program.

Learning Program Manager
The people in the organization responsible for the development, procurement, integration, modification, operation, maintenance, or final disposition of the elements of the Learning Program(s). In some organizations, there will be multiple iterations of Learning Programs where cybersecurity and privacy are managed separately.

Learning Program Plan
A formal document that provides an overview of an agency's cybersecurity and privacy Learning Program, including a description of the structure of the Learning Program, the resources dedicated to the Learning Program, the role of senior agency officials and staff, and the strategic goals and objectives of the Learning Program as a control planned for meeting applicable privacy requirements and managing privacy risks.

literacy
An individual's familiarity with a basic set of knowledge.

manageability
Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.

needs assessment
The process of identifying gaps in learning and the needs of learning activities.

predictability
Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service.

privacy event
The occurrence or potential occurrence of problematic data actions.

privileged network account
A network account with elevated privileges which is typically allocated to system administrators, network administrators, DBAs, and others who are responsible for system/application control, monitoring, or administration functions.

privileged user
A user who is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform. This may include special access to software applications or web publishing and will require additional training and the signing of an acceptable use policy. A user with a privileged account.

problematic data action
A data action that could cause an adverse effect for individuals.

program metrics
Tools designed to facilitate decision-making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data.

role-based training (RBT)
A multi-step process in the Learning Program that begins with defining the significant cybersecurity or privacy work roles in the organization, as well as the personnel aligned to the designated work role. The learning material is then assigned, acquired, or developed based on the tasks necessary to perform the work role. (See the NICE Framework [3] for "work role".)

> *NOTE:* In addition, NIST SP 800-53 control AT-3 [8] provides the following on Role-Based Training:
> Comprehensive role-based training addresses management, operational, and technical roles and
> responsibilities covering physical, personnel, and technical controls. Role-based training also includes
> policies, procedures, tools, methods, and artifacts for the cybersecurity and privacy roles defined.
> Organizations provide the training necessary for individuals to fulfill their responsibilities related to
> operations and supply chain risk management within the context of organizational cybersecurity and
> privacy programs. Role-based training also applies to contractors who provide services to federal agencies.

significant cybersecurity or privacy responsibilities

The preferred terminology herein for identifying those whose roles in the organization necessitate ongoing role-based training. These individuals have work-related responsibilities beyond those of All Users and will need to participate in general as well as specialized Learning Program activities.

> *NOTE:* From FISMA FY2014 CIO Metrics [12]: Those with significant cybersecurity responsibilities include all users who have one or more privileged network user account and all other users who have managerial or operational responsibilities that allow them to increase or decrease cybersecurity.

synchronous training

Training in which instructors and students are scheduled to participate together, whether it is in a virtual or a physical classroom-based learning environment.

tabletop materials

Materials designed for a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

> *NOTE*: From NIST SP 800-84, Tabletop exercises typically include the following documentation:
>
> o   Briefing. A briefing is created for the participants; it includes an agenda and logistics information.
>
> o   Facilitator Guide. The facilitator guide includes the following:
>
> – The purpose for conducting the exercise
>
> – The exercise's scope and objectives
>
> – The exercise's scenario, which is a sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives
>
> – A list of questions regarding the scenario that address the exercise objectives14
>
> – A copy of the IT plan being exercised.
>
> The types of questions documented in the facilitator guide should be tailored to the participants. For example, if senior-level personnel are the participants, the questions should be of a more general, high-level nature and focus on decision-making and oversight, which are consistent with their roles and responsibilities within the plan. If operational personnel are the participants, the questions should typically be focused on specific procedures and processes that are followed to carry out roles and responsibilities.
>
> o   Participant Guide. The participant guide includes the same information as the facilitator guide without the list of questions. Participant guides contain a modified, shorter list of questions to orient participants to the types of issues that may be discussed during the exercise.
>
> o   After Action Report.

training

Instruction to enhance the employee's capacity to perform specific job functions and tasks. It is a learning activity that focuses on skills, concepts, knowledge, and attitudes related to performing a job. It is designed to change what employees know and how they work.

> *NOTE:* References to training in US law: See U.S. Code § 4101 – Definitions [14]: (4) "training" means the process of providing for and making available to an employee, and placing or enrolling the employee in, a planned, prepared, and coordinated program, course, curriculum, subject, system, or routine of instruction or education, in scientific, professional, technical, mechanical, trade, clerical, fiscal, administrative, or other fields which will improve individual and organizational performance and assist in achieving the agency's mission and performance goals.

2232 **virtual-led**
2233 When instruction occurs in a virtual or simulated environment and is presented or facilitated by an instructor in real
2234 time.

2235 **warning banner**
2236 The opening screen that informs users of the implications of accessing a computer resource (e.g., consent to
2237 monitor); a security banner; system use notification.

2238 **web-based training**
2239 "Attendees" of an internet-based session can study independently and learn at their own pace. Testing and
2240 accountability features can be built-in to gauge performance. Web-based training can include video, audio, and
2241 interactive techniques, such as drag-and-drop or fill in the blank.

2242 **work role**
2243 A way of describing a grouping of work for which someone is responsible or accountable. Work Role names are not
2244 synonymous with job titles. Some work roles may coincide with a job title depending on an organization's use of job
2245 titles. Additionally, work roles are not synonymous with occupations. A single work role (e.g., Software Developer)
2246 may apply to those with many varying job titles (e.g., software engineer, coder, application developer). Conversely,
2247 multiple roles could be combined to create a particular job. This additive approach supports improved modularity
2248 and illustrates the fact that all learners in the workforce perform numerous tasks in various roles, regardless of their
2249 job titles. [3]